Contribuții la creşterea disponibilității, scalabilității şi securității sistemelor de comunicație

Valer BOCAN
e-mail: valer@bocan.ro

Conducător științific
prof. dr. ing. Vladimir CREȚU

Agenda

- Securitate, disponibilitate și scalabilitate în sisteme de comunicații
- Contribuții la creșterea disponibilității sistemelor de autentificare
- Contribuții la creșterea disponibilității rețelelor tip GSM
- Contribuții în domeniul sistemelor de distribuție digitală a conținutului
- Sumarul contribuțiilor

Scop

Scopul acestei lucrări de cercetare este de a prezenta soluții pentru ameliorarea disponibilității, scalabilității și securității sistemelor de comunicație.

Disponibilitate

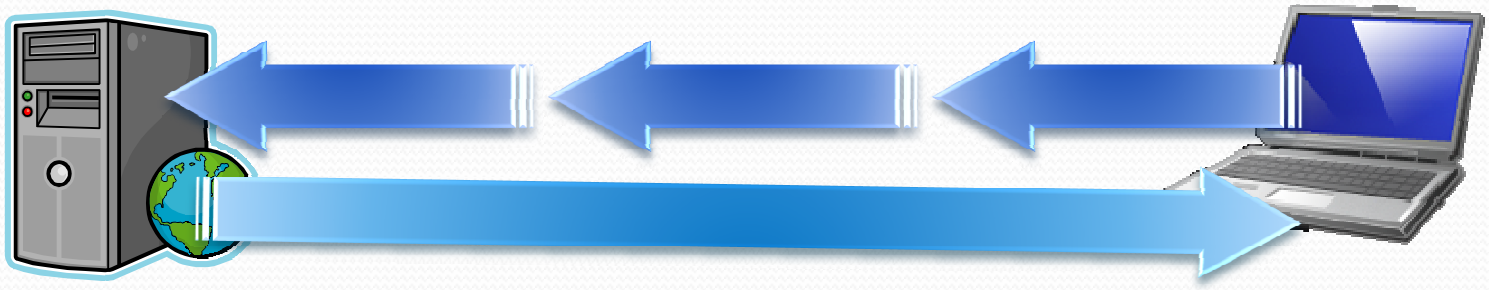
Scalabilitate

Securitate

Contribuții la creşterea disponibilității şi scalabilității sistemelor de autentificare

Threshold Puzzles
Adaptive Threshold Puzzles
Implementare în SSL
Detecția euristică a atacurilor DoS

Client Puzzles



Protocoalele de autentificare se bazează pe operații criptografice cu chei publice, scumpe ca timp de execuție.

Dezechilibrul între resursele alocate de client pentru execuția protocolului și cele alocate de server permite clientului să angajeze în mod repetat resurse importante ale serverului.

Client Puzzles

Creșterea artificială a costului pentru client prin tehnologia puzzles restabilește echilibrul părților.

« NS, k » — Generare

NS – valoare aleatoare unică (64 biți)
k – nivelul de dificultate al puzzle-ului

Rezolvare

h(C, NS, NC, X) = Y

h – funcție criptografică de dispersie (MD5, SHA1)
C – identitatea clientului
NS – valoarea aleatoare generată de server
NC – valoarea aleatoare generată de client
X – soluția puzzle-ului

Puzzle-ul propus în mod uzual este inversiunea prin forță brută a unei funcții hash cum ar fi MD5 sau SHA1.

Găsirea soluției este însă o operație paralelizabilă.

Threshold Puzzles

Limitarea superioară a nivelului de dificultate

Percepția dificultății puzzle-ului este optimă când:

$$\mathbf{T_{client} <= T_{server}}$$

$$\mathbf{T_{client} = M * t_c}$$

- M este numărul mediu de operații necesare pentru rezolvarea puzzle-ului, adică ~ 2^{k-1}.
- t_c este timpul mediu per operație.

$$\mathbf{T_{server} = Q * t_s}$$

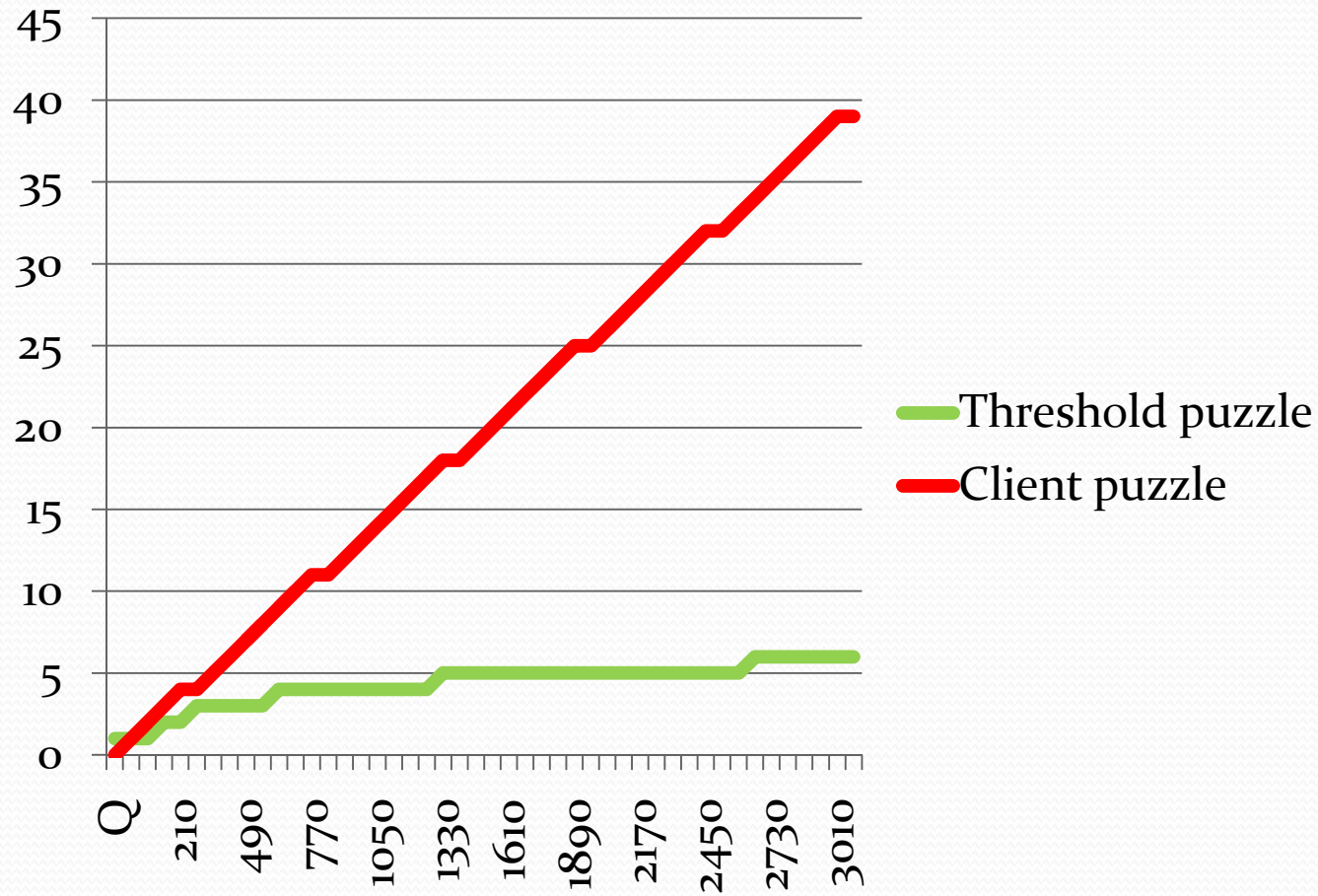
- Q este lungimea curentă a cozii de așteptare.
- t_c este timpul mediu per operație.

$$\mathbf{k <= \log_2 (\max(1, Q * t_s / t_c)) + 1}$$

Threshold Puzzles

$t_s = 0{,}003$

$t_c = 0{,}5$



Threshold Puzzles

Stabilirea unui timp minim de răspuns

Generare

« NS, t_o, k »

NS – valoare aleatoare unică (64 biți)
t_o – momentul generării puzzle-ului
k – nivelul de dificultate al puzzle-ului

Rezolvare

t_1, h(C, NS, NC, X) = Y

t_1 – momentul primirii soluției de către server
h – funcție criptografică de dispersie (MD5, SHA1)
C – identitatea clientului
NS – valoarea aleatoare generată de server
NC – valoarea aleatoare generată de client
X – soluția puzzle-ului

Condiția timpului minim de răspuns

$t_1 - t_o >= T_{estimat}$

$T_{estimat} = (2^{k-1}) * T_{operație}$

$T_{estimat}$ – timpul estimat pentru rezolvarea puzzle-ului
k – nivelul de dificultate al puzzle-ului
$T_{operație}$ – timpul minim de efectuare a unei operațiuni criptografice

Adaptive Threshold Puzzles

« **NS, t_o, k_c** »

Generare

NS – valoare aleatoare unică (64 biți)
t_o – momentul generării puzzle-ului
k_c – nivelul personalizat de dificultate al puzzle-ului

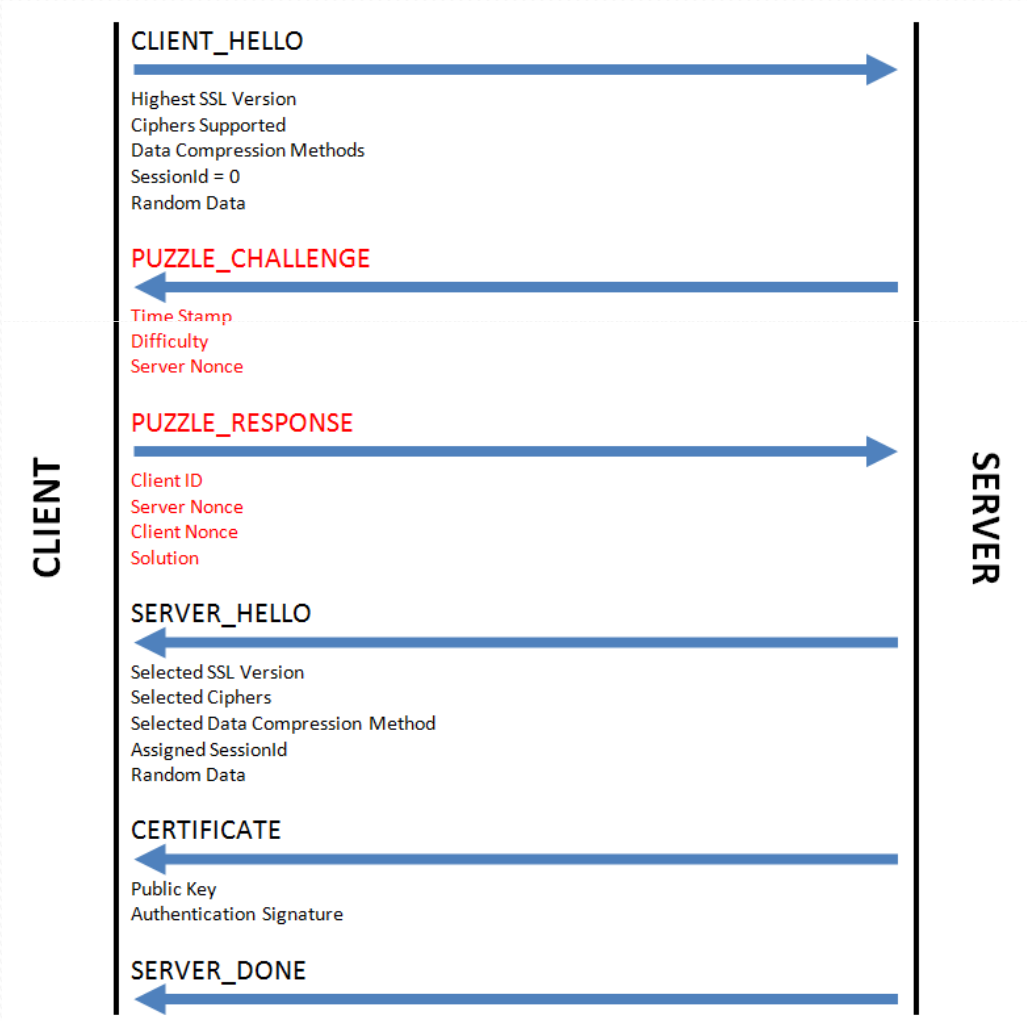
Dificultate adaptată fiecărui client

Pentru a evita blocarea clienților cu putere de calcul redusă (PDA, mobil, etc.), nivelul de dificultate se ajustează conform cu puterea de calcul raportată.

$$k_c = [k * \log_2(P_c/P_{ref})]$$

Unde:
P_{ref} – Puterea de calcul de referință
k – Dificultatea de referință (corelată cu Pref)
P_C – Puterea de calcul raportată de un client
k_C – Dificultatea pentru clientul în cauză

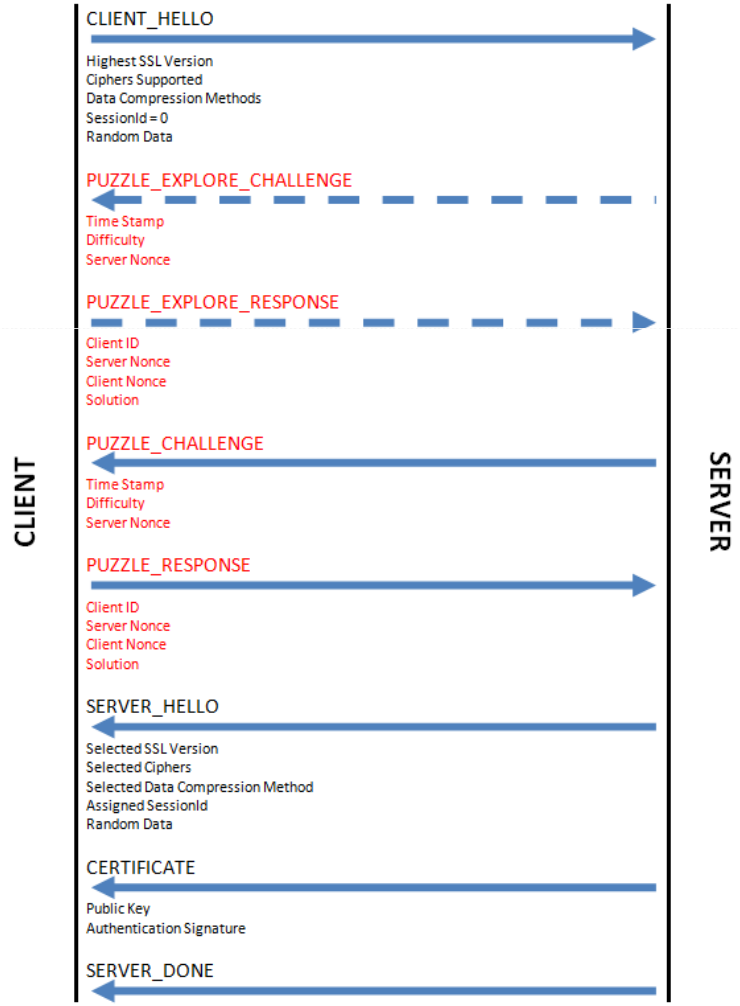
SSL cu Threshold Puzzles



Mesajul PUZZLE_CHALLENGE transmite parametrii NS și k, pe baza cărora clientul calculează răspunsul la puzzle.

Răspunsul clientului este trimis serverului în mesajul PUZZLE_RESPONSE.

SSL cu Adaptive Threshold Puzzles

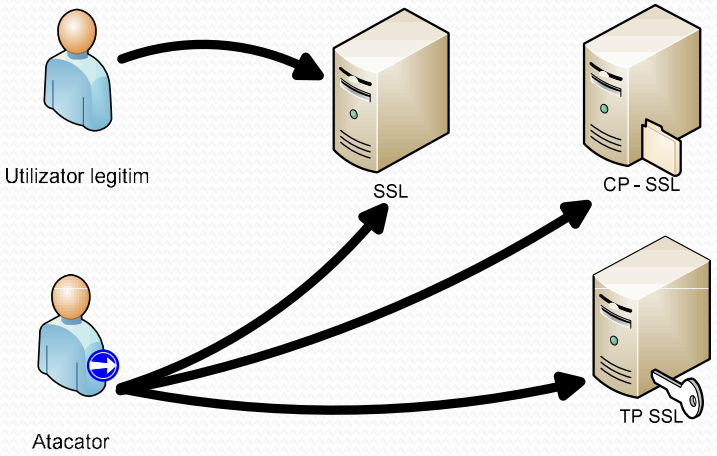


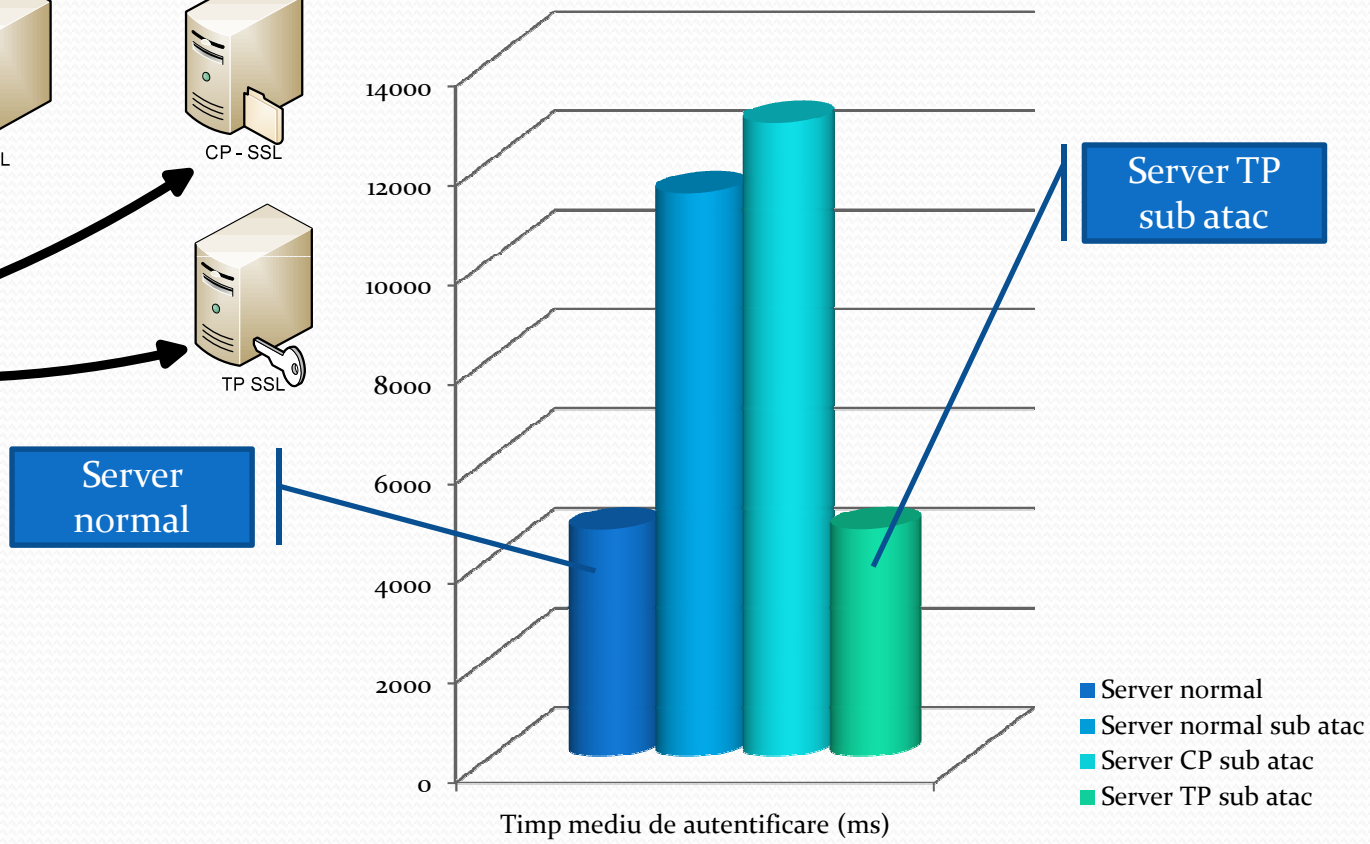
Mesajul **PUZZLE_EXPLORE_CHALLENGE** prezintă spre rezolvare clientului un puzzle cu o dificultate ușor crescută pentru a-i determina puterea de calcul și a calibra dificultatea viitoarelor puzzle-uri. Răspunsul clientului vine în mesajul **PUZZLE_EXPLORE_RESPONSE**.

Mesajul **PUZZLE_CHALLENGE** transmite parametrii NS și k, pe baza cărora clientul calculează răspunsul la puzzle.

Răspunsul clientului este trimis serverului în mesajul **PUZZLE_RESPONSE**.

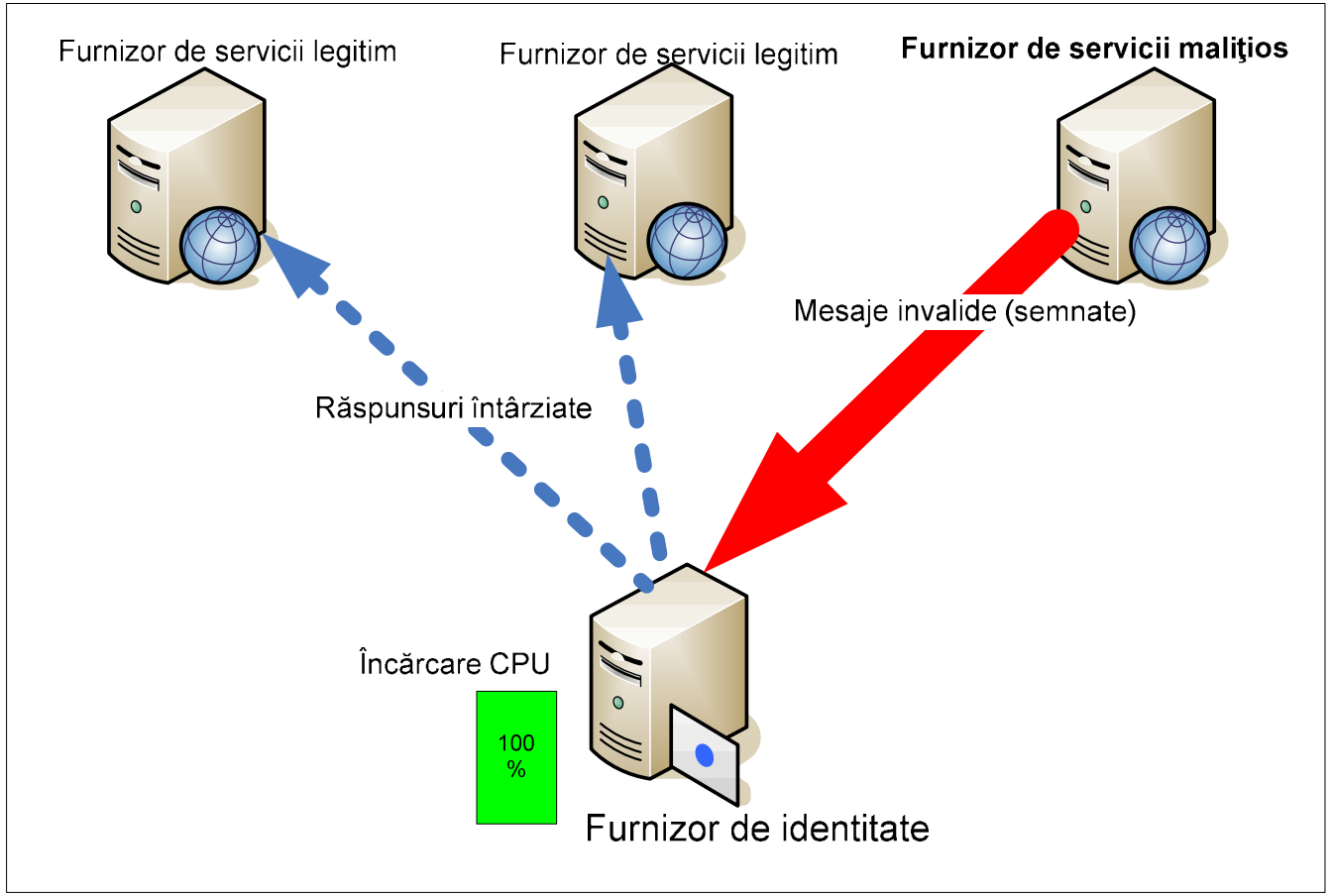
Rezultate comparative





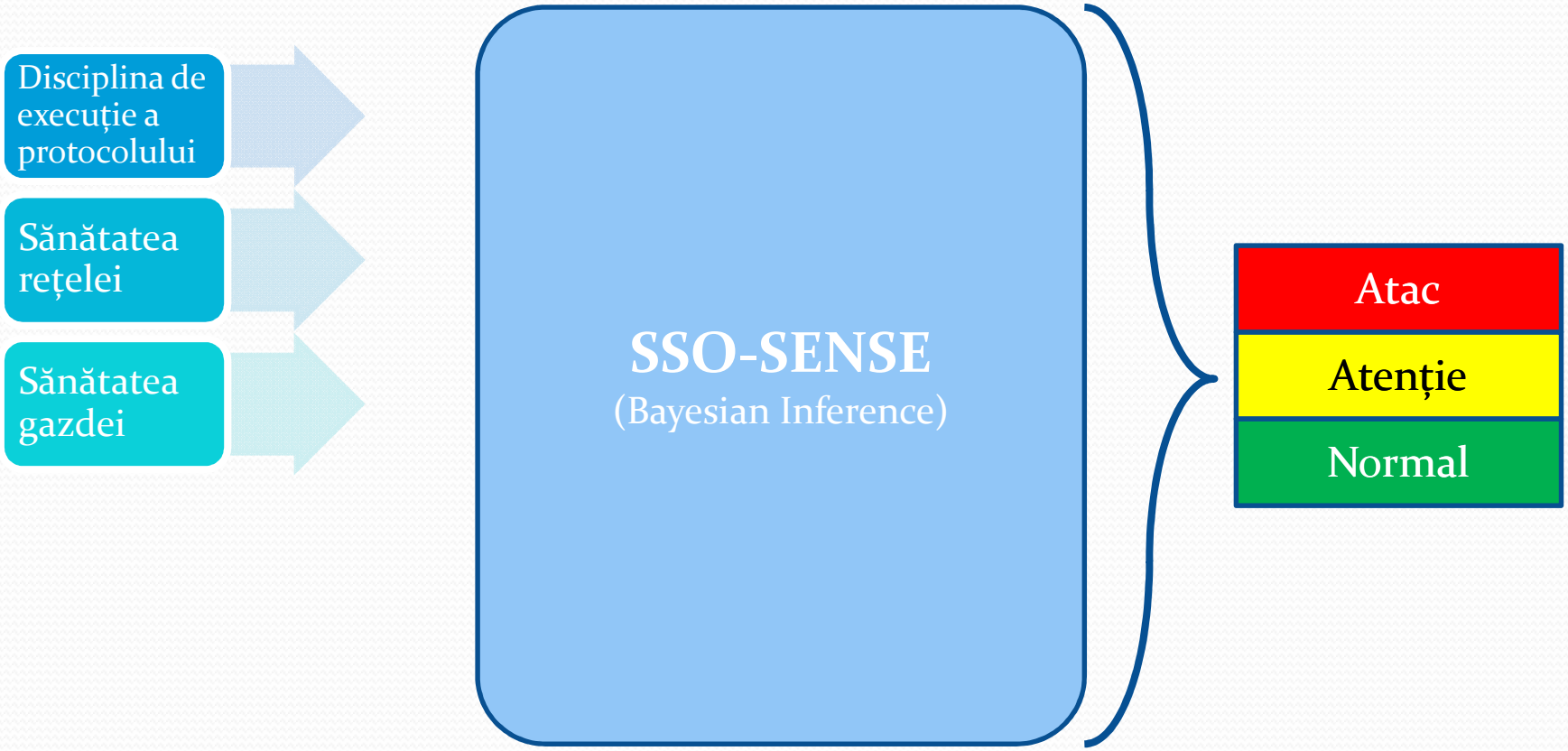
Detecția euristică a atacurilor DoS

Descoperirea unui atac în desfășurare este importantă pentru server care poate lua măsuri pentru conservarea resurselor sale.



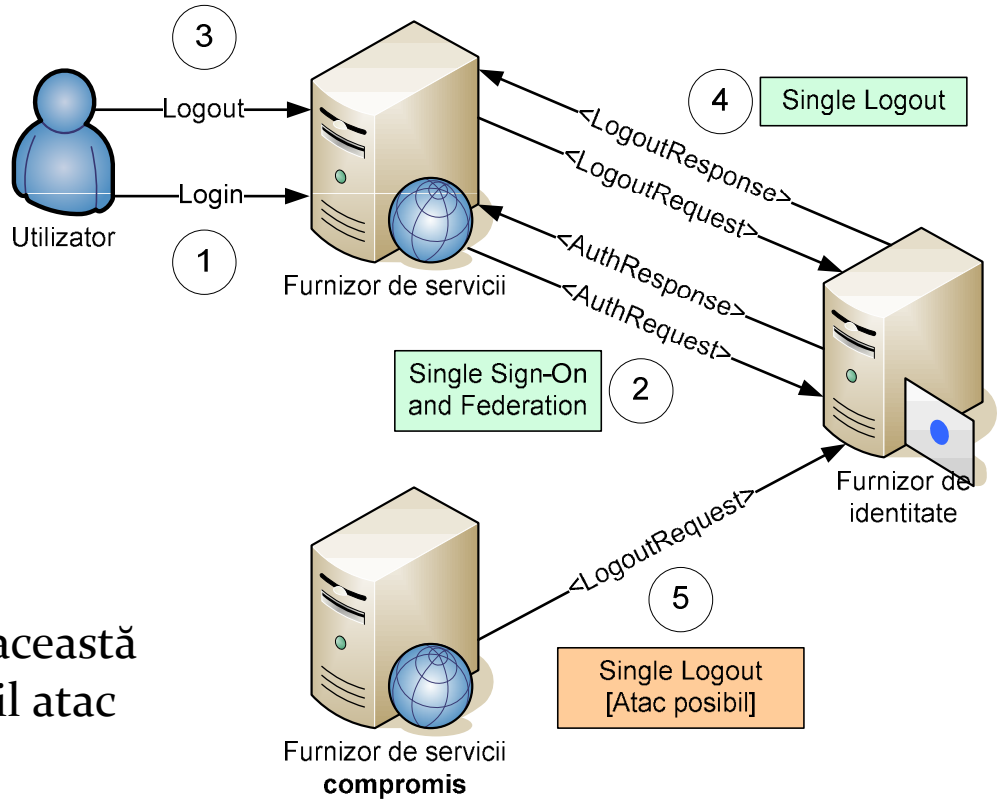
Detecția euristică a atacurilor DoS

Senzorii software de strâng informații din diverse puncte ale sistemului care sunt apoi agregate de motorul SSO-SENSE.



Detecția euristică a atacurilor DoS

Disciplina de execuție a protocolului



Execuția trebuie să urmeze o ordine stabilită de protocol, abaterea de la această ordine putând fi semnul unui posibil atac asupra sistemului SSO.

Detecția euristică a atacurilor DoS

Sănătatea rețelei

- Anomalii în operarea rețelei
- Anomalii Flash Crowd
- Anomalii de abuz

Detecția euristică a atacurilor DoS

Sănătatea sistemului gazdă

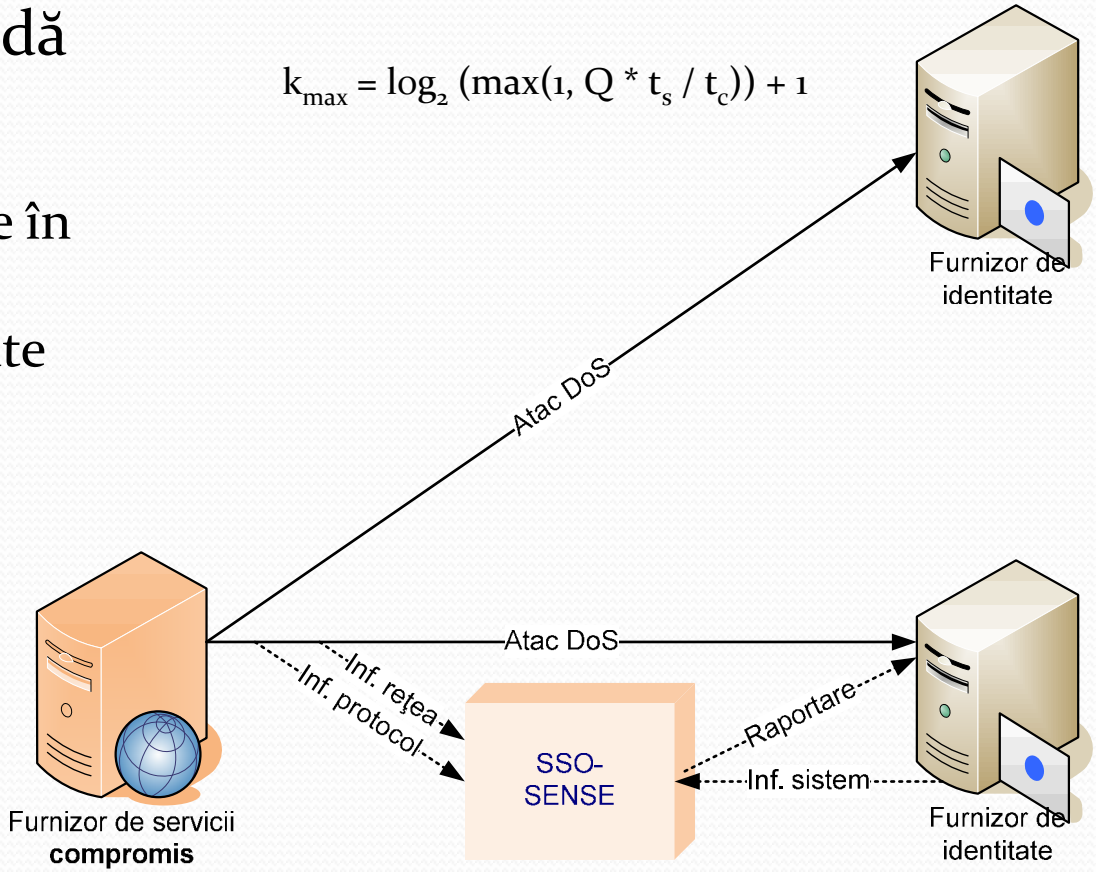
- Memorie disponibilă
- Încărcare curentă pe procesor
- Activitate I/O
- Rezerva de resurse a mașinii virtuale
- Stare drivere și servicii

Detecția euristică a atacurilor DoS

Sănătatea sistemului gazdă

$$k_{max} = \log_2 (\max(1, Q * t_s / t_c)) + 1$$

- **Stare normală** – complexitate în toată plaja [0; k_{max}].
- **Stare de atenție** – complexitate medie din plaja [0; k_{max}).
- **Stare de atac** – complexitatea maximă.



Implementare

1. Authentication Failure
2. Authentication Failure
3. Authentication Failure
4. Authentication Failure
5. Authentication Failure
6. Authentication Failure

```
Status before Authentication Failure:
Normal
Status after failure no. 1: Normal
Status after failure no. 2: Warning
Status after failure no. 3: Warning
Status after failure no. 4: Warning
Status after failure no. 5: Attack
Status after failure no. 6: Attack
```

Probabilitățile stabilite inițial pentru evenimente au fost:
H_1 (stare normală) = 0,9
H_2 (stare de atenție) = 0,09
H_3 (stare de atac) = 0,01

Sistemul este declarat sub atac după al 5-lea eveniment.

Implementare

1. Protocol failure
2. Protocol failure
3. Protocol failure
4. Protocol failure
5. Protocol failure
6. Protocol failure

Probabilitățile stabilite inițial pentru evenimente au fost:
H_1 (stare normală) = 0,9
H_2 (stare de atenție) = 0,09
H_3 (stare de atac) = 0,01

Sistemul este declarat sub atac după al 4-lea eveniment.

```
Status before Protocol Follow-up
Failure: Normal
Status after failure no. 1: Warning
Status after failure no. 2: Warning
Status after failure no. 3: Warning
Status after failure no. 4: Attack
Status after failure no. 5: Attack
Status after failure no. 6: Attack
```

Contribuții la creşterea disponibilității rețelelor GSM

Clasificarea vulnerabilităților GSM
Atacuri DoS în GSM
Tehnici de creştere a disponibilității

Clasificarea vulnerabilităților GSM

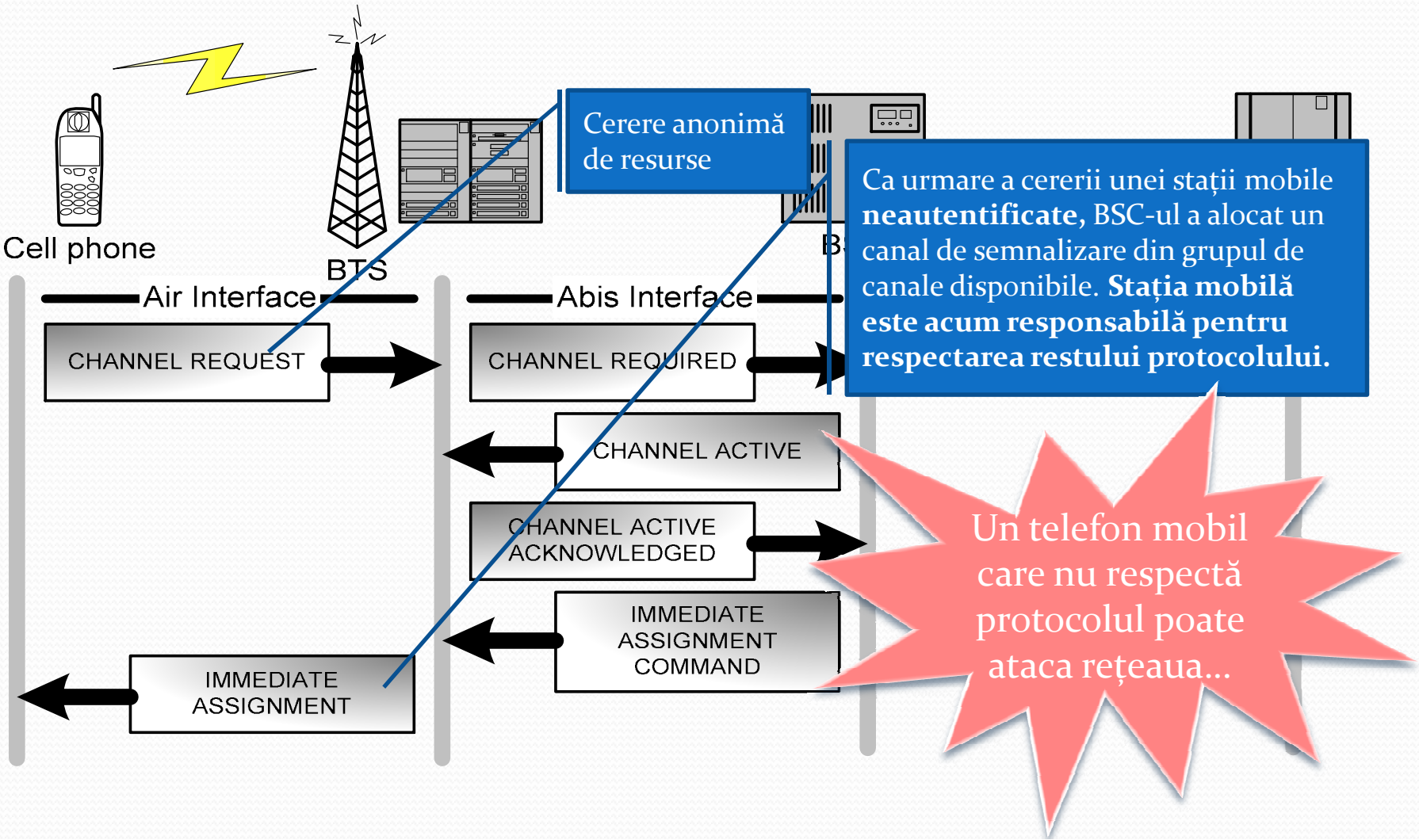
Clasificarea DREAD folosită inițial în software poate evalua gravitatea atacurilor de diverse tipuri asupra rețelelor GSM.

- Destroying Potential
- Reproducibility
- Exploitability
- Affected users
- Discovery Potential

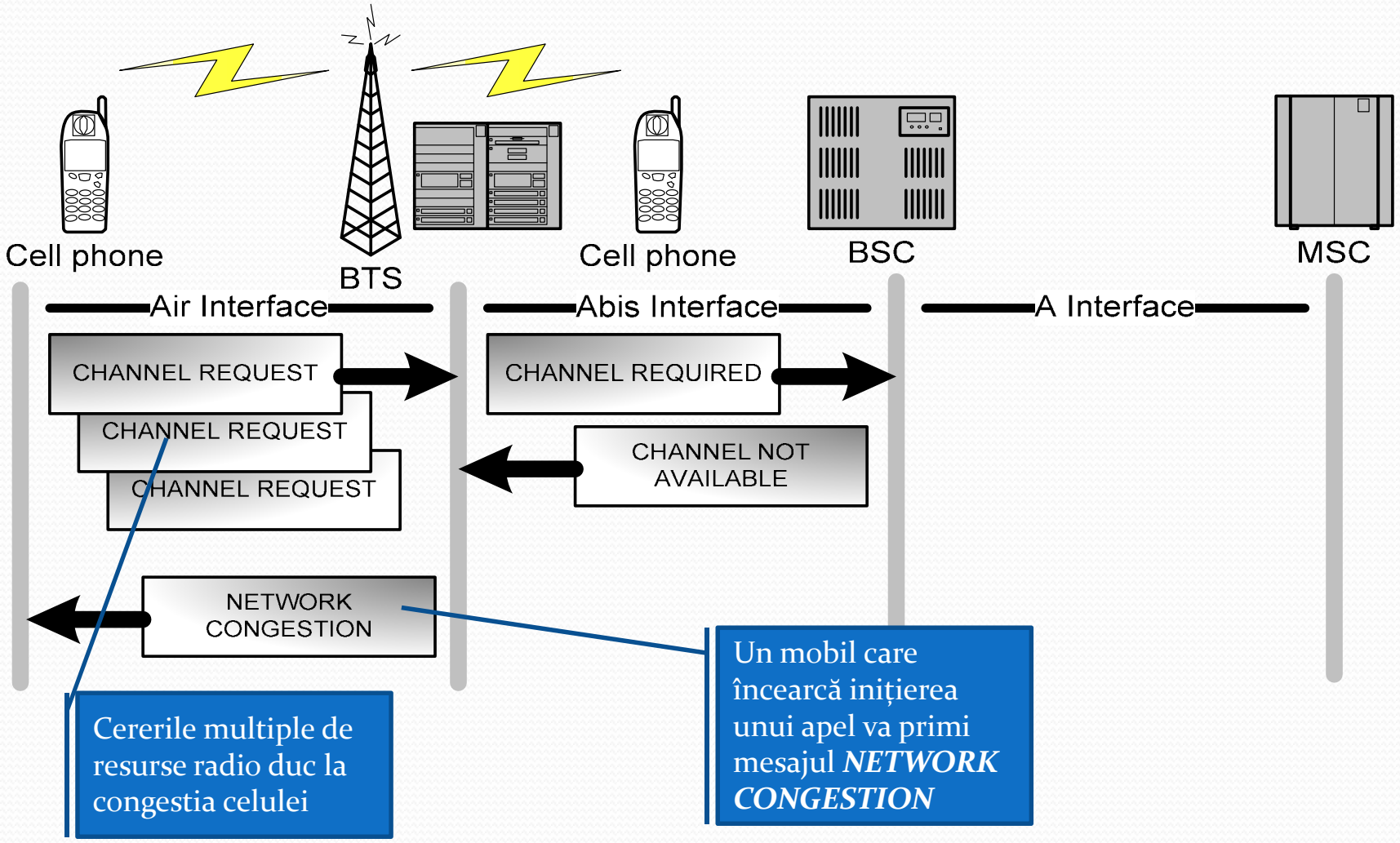
Clasificarea vulnerabilităților GSM

Vulnerabilitate	Scor de risc
Denial of Service Attacks	8.2
Hijacking outgoing calls in networks with encryption disabled	6
Hijacking outgoing calls in networks with encryption enabled	6
Hijacking incoming calls in networks with encryption disabled	6
Hijacking incoming calls in networks with encryption enabled	6
De-registration Spoofing	5.8
Location Update Spoofing	5.8
Camping on a False BTS	5.6
User impersonation through eavesdropped authentication response	5.6
Passive Identity Caching	5.2
Encryption Suppression	5.2
Active Identity Caching	5
Eavesdropping on User Data by Suppressing Encryption	5
Suppression of Encryption between Target User and True Network	5
Eavesdropping on User Data by Forcing the Use of a Compromised Key	5
User impersonation with compromised authentication vector	5
Compromised Cipher Key	4.8

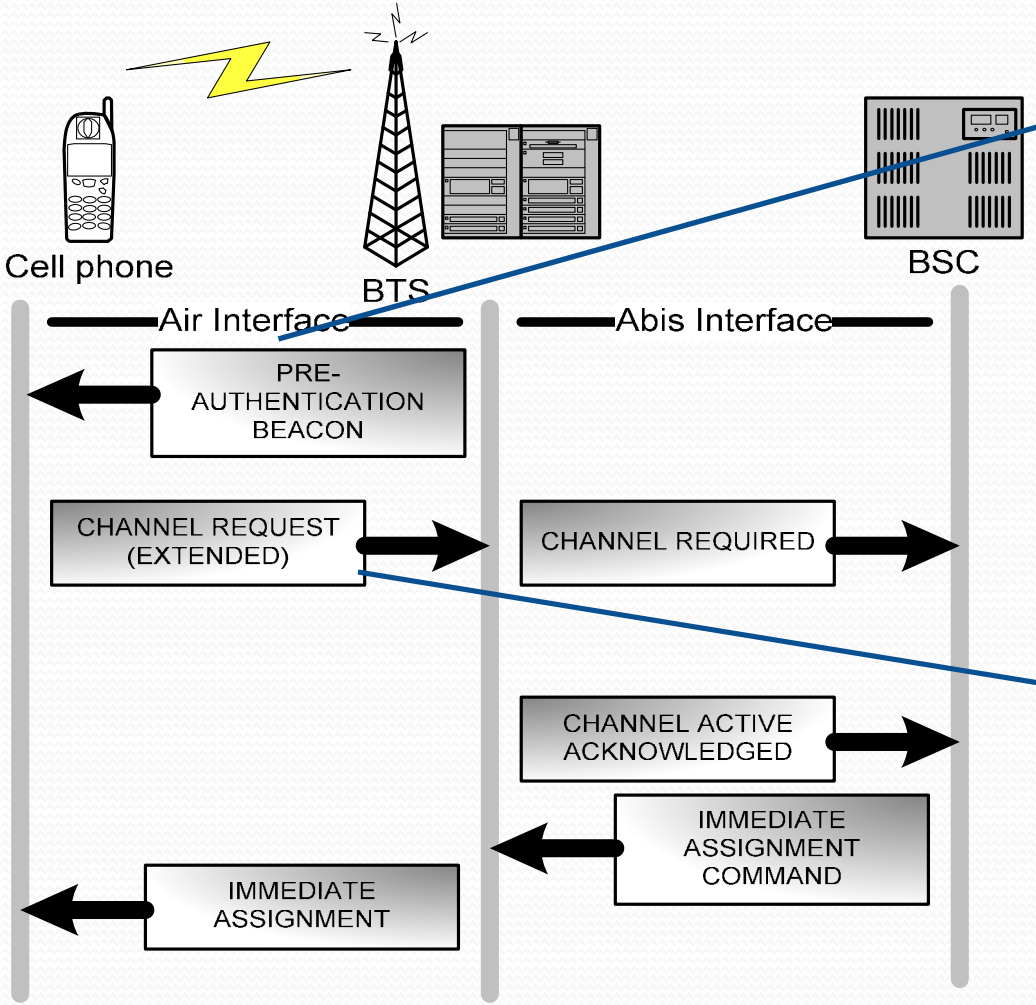
Atacuri DoS în GSM



Atacuri DoS în GSM



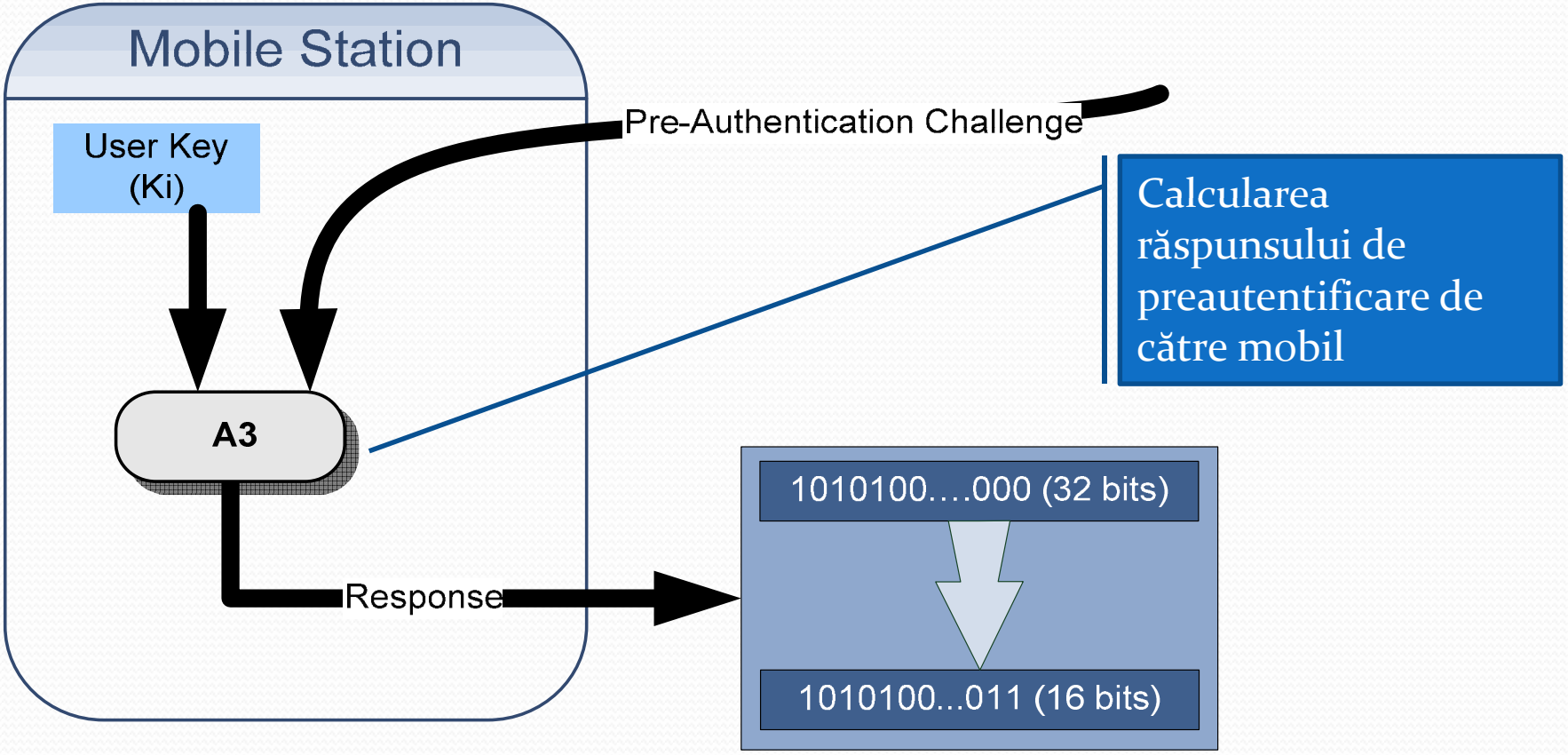
Preautentificarea clientului



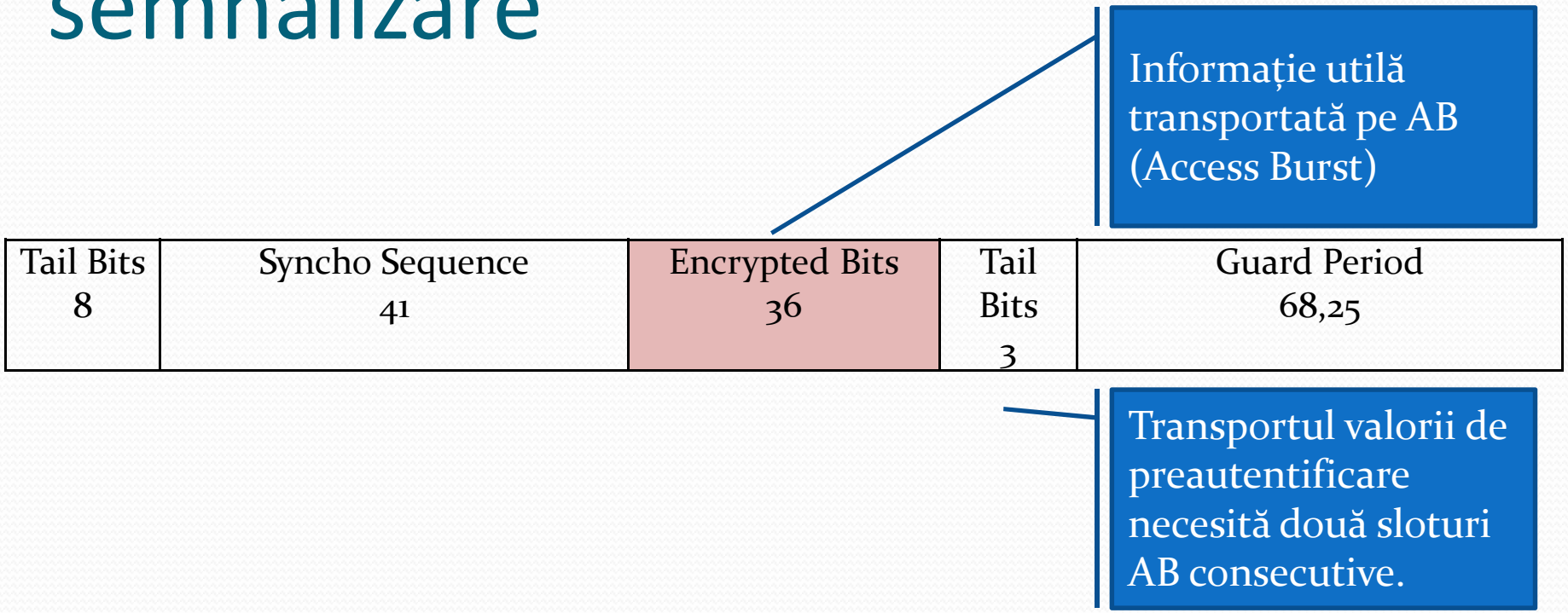
Baliza de preautentificare: Se transmite o valoare unică aleatoare pe 128 de biți

Valoarea aleatoare se combină cu cheia utilizator K_i de pe SIM, cu algoritmul A3.

Răspunsul de preautentificare



Impactul asupra capacității de semnalizare



Preautentificarea are ca rezultat înjumătățirea capacității de semnalizare la 109 accese RACH pe secundă.

Valoarea de preautentificare poate fi ghicită de un atacator în medie de 12 ori pe oră, la capacitatea maximă a canalului.

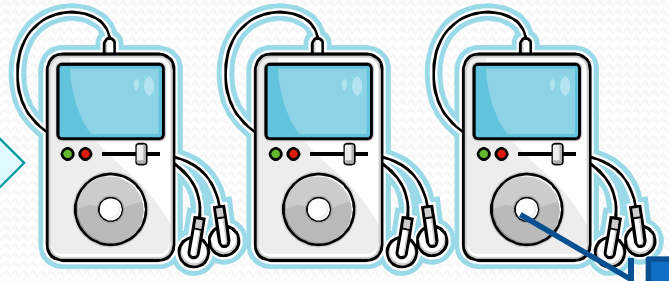
Contribuții în domeniul sistemelor de distribuție digitală a conținutului

Arhitectură scalabilă de distribuție digitală a conținutului

Distribuția scalabilă a conținutului digital

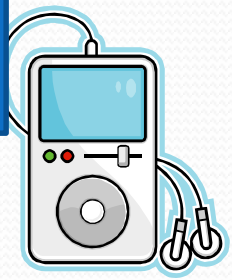
Același conținut digital se distribuie **simultan** clienților. Modalitatea de transfer permite o scalabilitate superioară altor abordări.

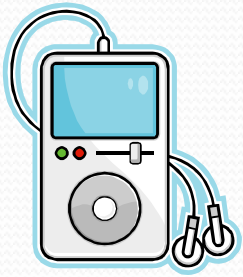
Distribuție



Redistribuția conținutului prin intermediari scade încărcarea pe server.

Redistribuție



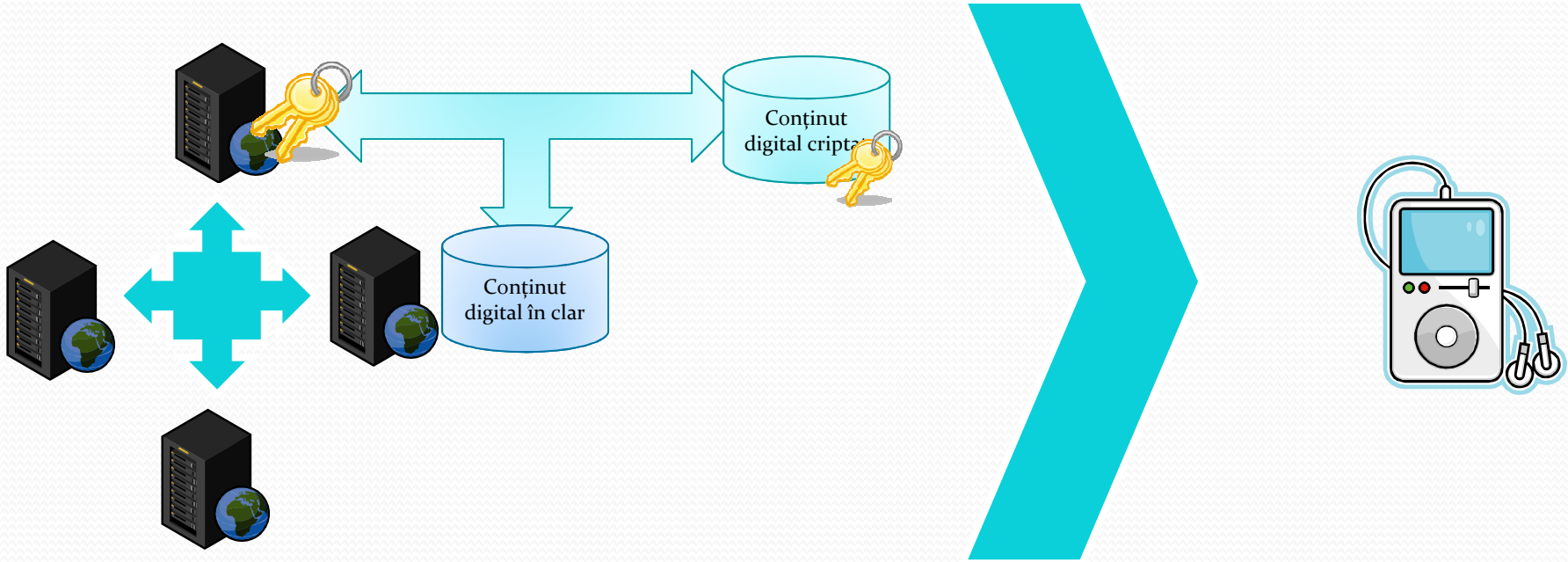


Înțelegerea securizată între deținătorii de copyright permite un audit exact.

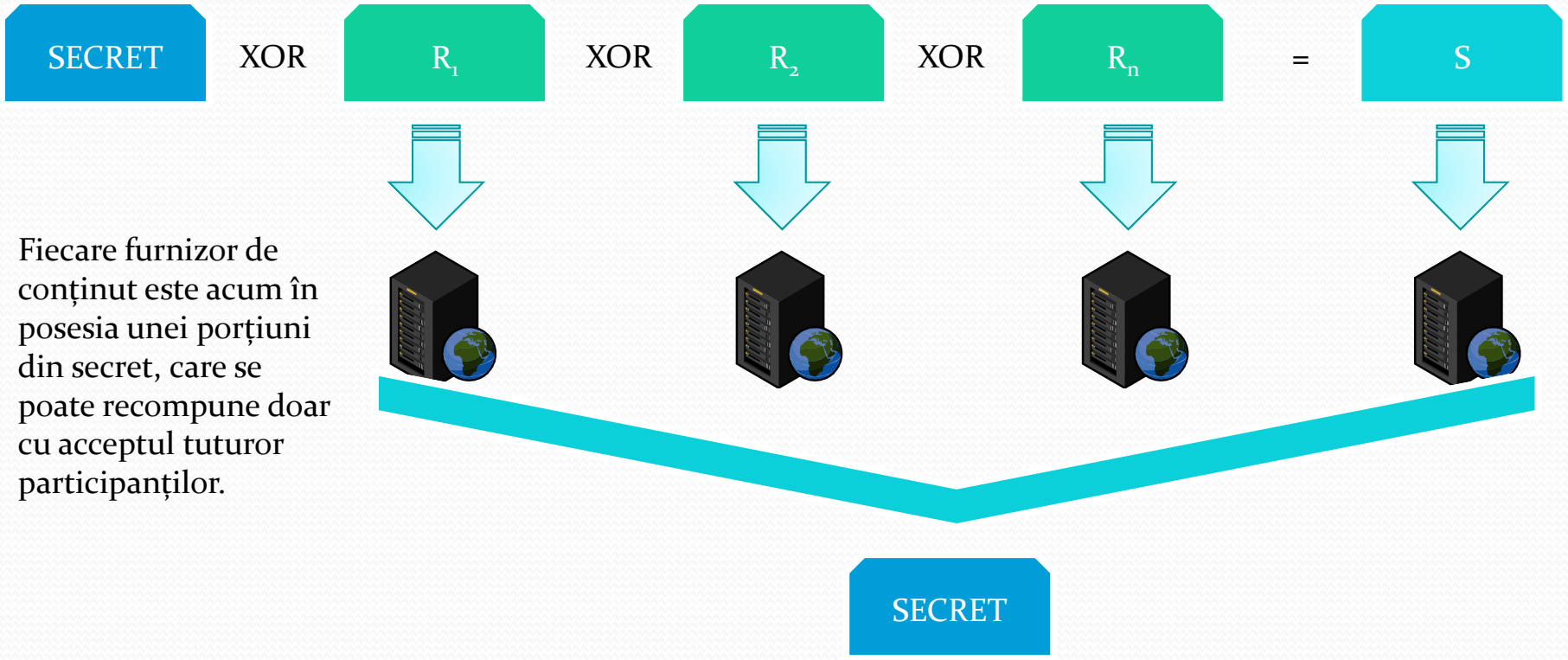
Distribuția conținutului

1. $C_1, C_2, ..., C_n \rightarrow CP_1$: Solicitare conținut
2. $C_1, C_2, ..., C_n \leftrightarrow CP_1$: Autentificare reciprocă
3. $CP_1 \leftrightarrow CP_2, ..., CP_n, MCP$: Acord asupra drepturilor de distribuție
4. $C_1, C_2, ..., C_n \leftrightarrow CP_1$: Plată (pas opțional)
5. $CP_1 \rightarrow C_1, C_2, ..., C_n : [M]K, [K]eS, X, \eta, \delta, \Lambda$

X – lacăt
K – cheie simetrică temporară
eS – cheie de sesiune
η – drepturi de redare și redistribuție
δ – metadata
$\Lambda = [h(M, \eta, \delta, X)]_{dCP}$ - licența pentru conținut



Cooperarea furnizorilor

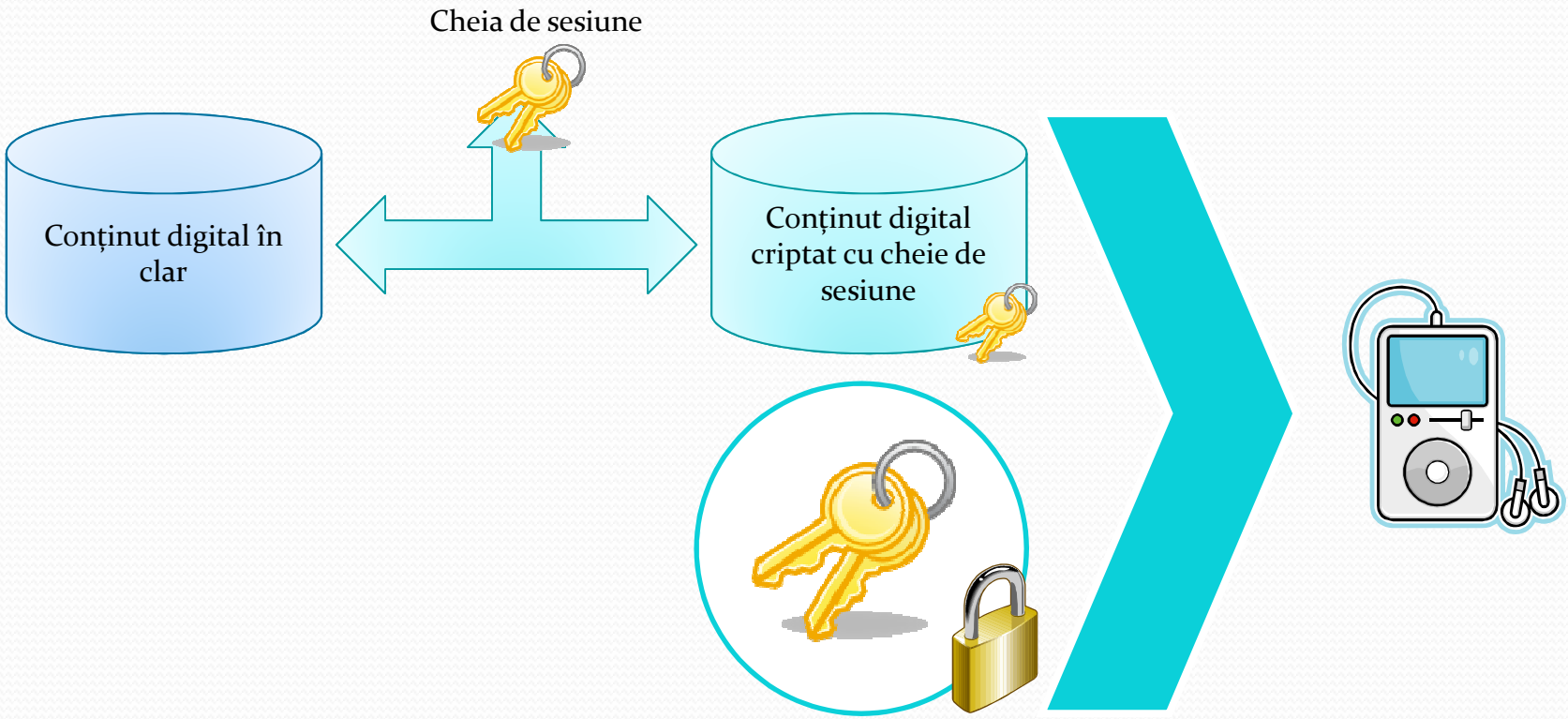


Fiecare furnizor de conținut este acum în posesia unei porțiuni din secret, care se poate recompune doar cu acceptul tuturor participanților.

Secretul recompus prin votul părților este arbitrat de o entitate în care toată lumea are încredere (MCP – Master Content Provider).

Difuzare securizată

Conținutul digital este criptat o singură dată folosind o cheie de sesiune, apoi este trimis clientului cu o cheie de decriptare. Aceasta este protejată cu un lacăt generat prin teorema chineză a restului (CRT – Chinese Remainder Theorem).



Difuzare securizată

Se dă un grup de n clienți notat C, format din C_1, C_2, ..., C_n, fiecare având o cheie privată e_i, respectiv una publică d_i, precum și un set de n numere pozitive întregi N_1, N_2, ..., N_n cu proprietatea că sunt numere prime între ele și sunt cunoscute public în sistem.

Din grupul C, un subset de k clienți ($k \geq 2$) solicită același conținut digital de la furnizorul de conținut (CP). Dacă în continuare considerăm un set de k întregi pozitivi R_1, R_2, ... R_n, avem sistemul de congruențe:

$$\begin{cases} X \equiv R_1 \pmod{N_1} \\ X \equiv R_2 \pmod{N_2} \\ \dots \\ X \equiv R_k \pmod{N_k} \end{cases}$$

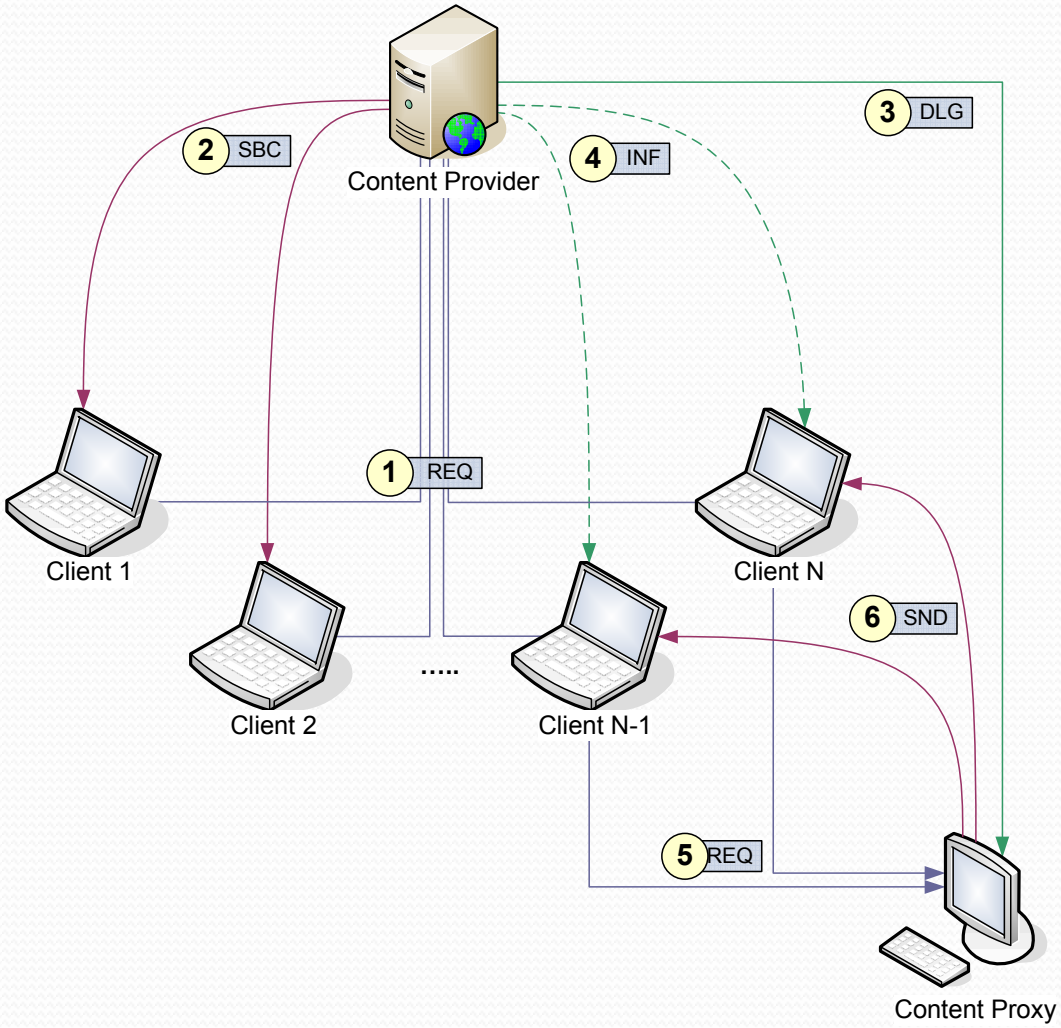
Soluția comună X este dată de ecuația:

$$X = \left(\sum_{i=1}^{k} \frac{L}{N_i} \cdot R_i \cdot f_i\right) \bmod L$$

$$1 \equiv f_i \cdot \frac{L}{N_i} \bmod N_i$$

$$L = \prod_{i=i}^{k} N_i$$

Retransmisia conținutului



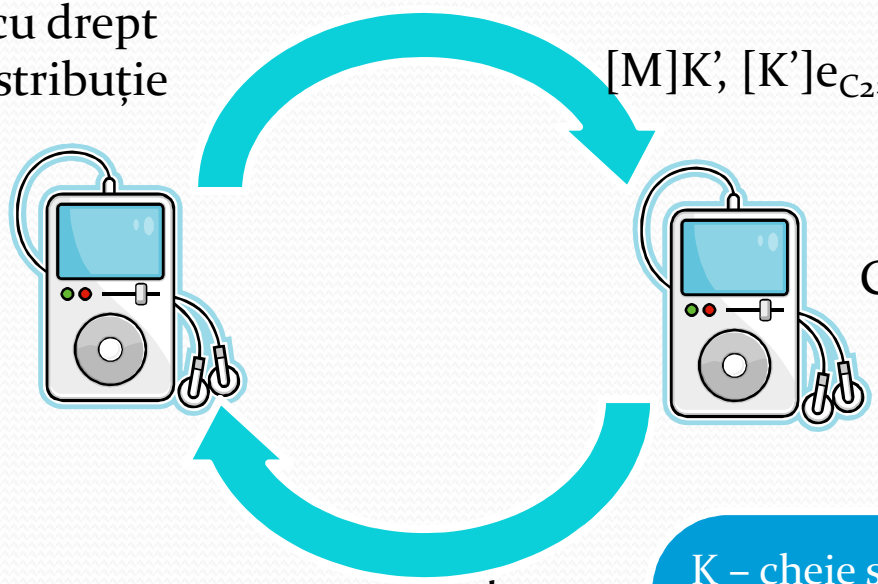
Conținutul digital destinat unui grup de clienți poate fi retransmis de către entități care nu au drepturi de redare, fără ca acestea să poată avea acces la conținutul în clar.

Serverul este eliberat rapid de sarcina de transmisie a conținutului, aceasta fiind preluată de clienți de tip proxy.

Redistribuția conținutului

Client cu drept de redistribuție

$[M]K', [K']e_{C_2}, \eta, \eta', \delta, \Lambda, \Lambda'$



Client destinație

ϕ

K – cheie simetrică temporară
eS – cheie de sesiune
η, η' – drepturi de redare și redistribuție
δ – metadata
$\Lambda = [h(M, \eta, \delta, X)]_{dCP}$ - licența pentru conținut
$\Lambda' = [h(e_1, e_2, M, \eta', \delta, X)]_{dC_1}$ - noua licență pentru conținut
$\phi = [h(eC_1, eCP, [M]K', \delta, \eta']_{dC_2}$

Metrica de evaluare

Timpul total de distribuție este:

$$T_{dist} = \sum_{i=1}^{N} Tsk_i + \sum_{i=1}^{N} Tce_i + \sum_{i=1}^{M} Tx_i + \sum_{i=1}^{N} Tsend_i$$

Unde:

- T_{dist} – Timpul total necesar pentru a transmite toate instanțele conținutului
- T_{sk} – Timpul necesar pentru a genera cheia de sesiune
- T_{ce} – Timpul necesar pentru a cripta conținutul cu cheia de sesiune
- T_x – Timpul necesar pentru a general lacătul C sau pentru a cripta cheia de sesiune cu cheia publică a receptorului (în cazul redistribuției)
- T_{send} – Timpul necesar pentru a transmite o instanță a conținutului către client
- N – Numărul de instanțe ale conținutului care trebuie transmise
- M – Numărul de clienți la care conținutul trebuie transmis

Broadcast

$$T_{broadcast} = Tsk + Tce + \sum_{i=1}^{M} Tx_i + Tsend$$

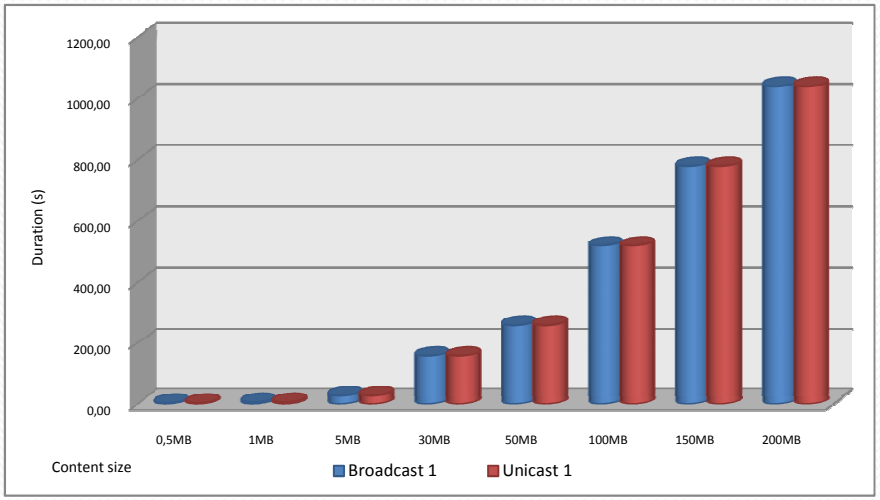
(Numărul instanțelor de conținut care trebuie transmise este N = 1)

$$T_{unicast} = \sum_{i=1}^{N} (Tsk_i + Tce_i + Tx_i + Tsend_i)$$

(Numărul de instanțe ale conținutului care trebuie transmise este egal cu numărul clienților, astfel încât N = M)

Unicast

Performanță comparativă

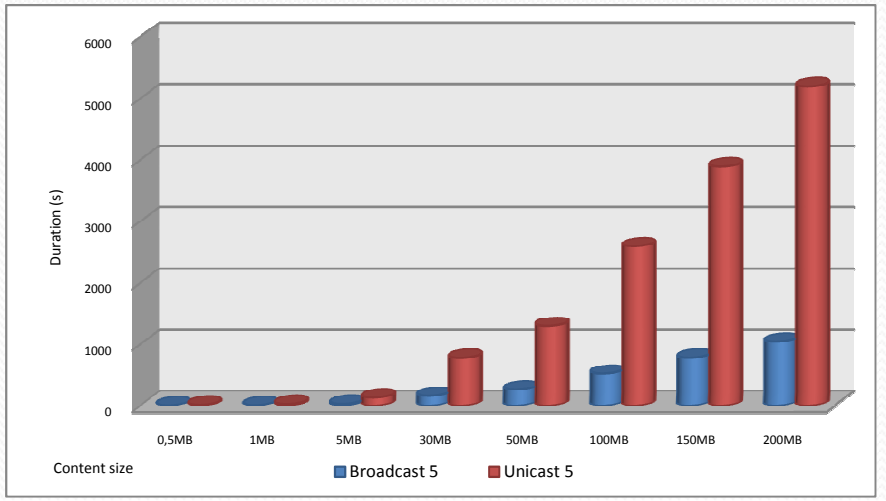


Comparație broadcast-unicat pentru 1 client

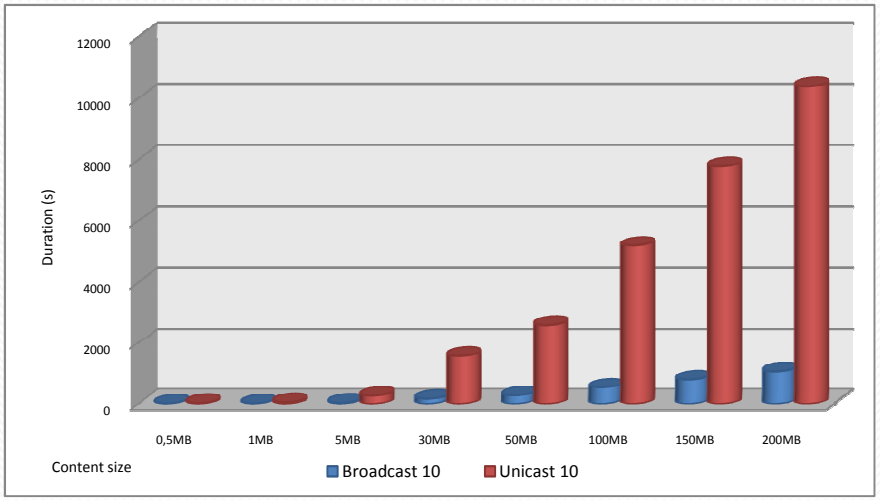
Timpul de distribuție este practic același, nu se observă un câștig de performanță pentru modelul broadcast.

Comparație broadcast-unicat pentru 5 clienți

Odată cu creșterea numărului de clienți deserviți simultan, câștigul de performanță pentru modelul broadcast este evident.

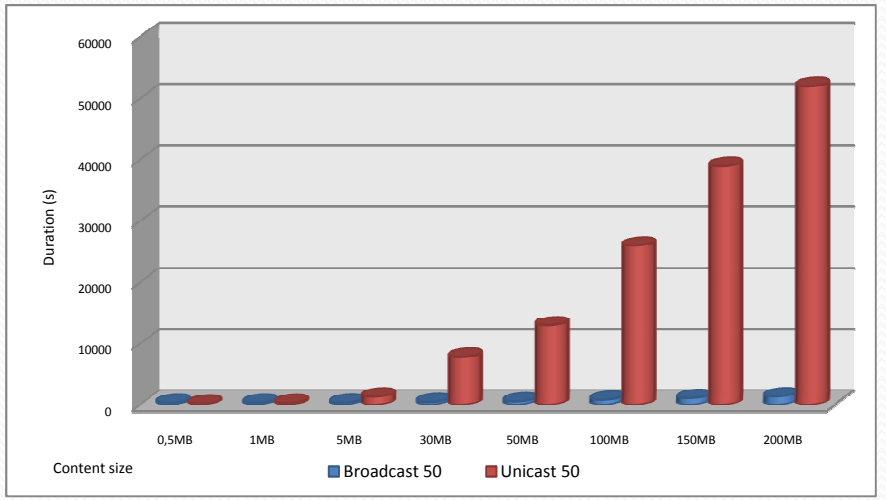


Performanță comparativă



Comparație broadcast-unicat pentru 10 clienți

Comparație broadcast-unicat pentru 50 clienți



Sumarul contribuțiilor

Domeniul de interes al lucrării

Securitatea și buna funcționare a sistemelor de comunicație este o problemă de primă importanță, de aceea lucrarea acoperă un spectru larg:

- Sistemele de autentificare
- Sistemele de tip Single Sign-On (SSO)
- Rețelele de comunicație mobilă de tip GSM
- Sistemele de distribuție a conținutului digital

Contribuții

- Au fost dezvoltate tehnologiile Threshold Puzzles și Adaptive Threshold Puzzles, pentru a acoperi situațiile în care tehnologia Client Puzzles nu este eficientă.
- S-au introdus două versiuni ale schimbului de mesaje Handshake din cadrul protocolului SSL, astfel încât acesta să suporte tehnologiile Threshold Puzzles și Adaptive Threshold Puzzles.
- S-a evidențiat posibilitatea ca atacurile DoS să fie detectate cu o anumită probabilitate înainte ca acestea să aibă loc prin aplicarea inferenței bayesiene.
- S-a introdus SSO-Sense, un modul de estimare euristică a nivelului de risc pentru sistemele de autentificare.

Contribuții

- Vulnerabilitățile sistemului GSM au fost evaluate cu o metodă de clasificare numită DREAD.
- S-a arătat cauza pentru care sistemul GSM este vulnerabil la atacuri DoS (lipsa preautentificării).
- S-a arătat de asemenea că un singur atacator este capabil de a dezactiva o întreagă celulă GSM și în anumite cazuri chiar și celulele adiacente.
- Deoarece nu sunt implicate costuri financiare (nu se efectuează nici un apel în sine), costul efectiv al lansării un atac devastator este zero din punctul de vedere al plăților către operatorul vizat.
- S-a propus introducerea preautentificării terminalelor GSM în cazul inițierii unui apel de către acestea.

Contribuții

- S-a introdus o arhitectură de distribuție a conținutului digital cu următoarele avantaje:
  - **Scalabilitate** – Sistemului de broadcast propus deservește simultan un număr de clienți cu cereri similare, acumulate la intervale de timp prestabilite.
  - **Distribuție asincronă** –Fluxul digital poate fi difuzat (broadcast) prin rețea fără a exista pericolul ca un client neautorizat să-l poată reda. Sarcina de distribuție poate fi preluată cu succes de către orice clienți aflați mai aproape de receptor.
  - **Colaborare între deținătorii de copyright** –Arhitectura propusă este capabilă să partajeze drepturile asupra conținutului prin tehnica „secret spliting” și să ofere acces fizic la acesta doar când participanții sunt cu toții de acord.

Publicații

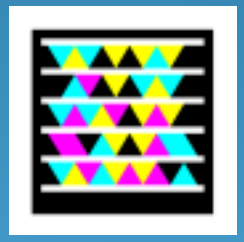
- **Valer BOCAN, Vladimir CREȚU** - *SCADDIC: The Implementation and Performance of a Scalable and Secure Architecture for Digital Content Distribution*, 7th Conference on Communications, Military Technical Academy, Bucharest, 2008
- **Valer BOCAN, Vladimir CREȚU** - *Threats and Countermeasures in GSM Networks*, Journal of Networks, Academy Publishers, ISSN 1796-2056
- **Valer BOCAN, Mihai FĂGĂDAR-COSMA** - *Scalable and Secure Architecture for Digital Content Distribution*, SoftCOM 2006 - International Conference on Software, Telecommunications and Computer Networks, Split, Croatia
- **Valer BOCAN, Vladimir CREȚU** - *Mitigating Denial of Service Threats in GSM Networks*, ARES 2006 - The First International Conference on Availability, Reliability and Security, Wien, Austria
- **Valer BOCAN, Mihai FĂGĂDAR-COSMA** - *Adaptive Threshold Puzzles,* EUROCON 2005 - The International Conference on "Computer as a tool", Belgrade, Serbia and Montenegro
- **Valer BOCAN, Mihai FĂGĂDAR-COSMA** - *Towards DoS-resistant Single Sign-On Systems*, EUROCON 2005 - The International Conference on "Computer as a tool", Belgrade, Serbia and Montenegro
- **Valer BOCAN** - *Sisteme Single Sign-On sub atacuri Denial-of-Service. Studiu de caz: Proiectul Liberty Alliance*, Referat de doctorat nr. 3, Politehnica University of Timisoara
- **Valer BOCAN** - *Studiu asupra nivelului de siguranta oferit de protocoalele de autentificare*, Raport de doctorat nr. 2, Politehnica University of Timisoara, 2004
- **Valer BOCAN** - *Developments in DoS Research and Mitigating Technologies,* CONTI 2004 - Periodica Politehnica, Transaction on Automatic Control and Computer Science Vol. 49 (63), 2004, ISSN 1224-600X
- **Valer BOCAN, Vladimir CREȚU** - *Security and Denial of Service Threats in GSM Networks*, CONTI 2004 - Periodica Politehnica, Transaction on Automatic Control and Computer Science Vol. 49 (63), 2004, ISSN 1224-600X
- **Valer BOCAN** - *Threshold Puzzles. The Evolution of DoS-Resistant Authentication*, CONTI 2004 - Periodica Politehnica, Transaction on Automatic Control and Computer Science Vol. 49 (63), 2004, ISSN 1224-600X
- **Valer BOCAN** - *Stadiul actual al dezvoltarii sistemelor de securitate pentru retele de calculatoare de inalta siguranta*, Raport de doctorat nr. 1, Politehnica University of Timisoara

Bibliografie selectivă

- Alcatel University – *Introduction to the Alcatel GSM Network*, 2003
- Emmanuel Gadaix – *GSM and 3G Security*, Black Hat Conference Singapore, 2001
- Ari Juels, John Brainard – *Client puzzles: A cryptographic defense against connection depletion attacks*, Proceedings of the NDSS 1999
- T. Aura, P. Nikander, J. Leiwo – *DOS-resistant authentication with client-puzzles*, Proceeding of the Cambridge Security Protocols Workshop 2000, LNCS, Cambridge, UK, 2000
- Ronald R. Rivest, Adi Shamir, David A. Wagner – *Time-lock Puzzles and Timed-release Cryptography*, 1996
- S. K. Nair, B. C. Popescu, C. Gamage, B. Crispo and A. S. Tanenbaum - "*Enabling DRM – preserving Digital Content Redistribution*", 7th International IEEE Conference on E-Commerce Technology, 2005

Vă mulțumesc

Teza de doctorat și prezentarea asociată (în format PDF) se găsesc la adresa **www.dataman.ro/publications**



Vezi această prezentare pe telefonul mobil sau PDA.
http://gettag.mobi

Vezi teza de doctorat pe telefonul mobil sau PDA.
http://gettag.mobi