How to Authenticate Unknown Principals without Trusted Parties

Based on a presentation originally given at

Tenth Cambridge Protocol Workshop,
April 17th, 2002, Cambridge, UK

Jari Arkko, Pekka Nikander
Ericsson NomadicLab, Finland

Presentation Outline

- Introduction
- Weak authentication toolbox
- Weak authentication methods
- Modelling the impacts
- Conclusions

Introduction to Weak Authentication

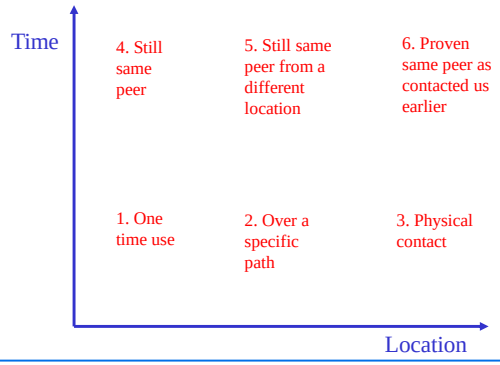
"Weak Authentication" (WA) means cryptographic authentication between previously unknown parties without relying on trusted third parties.

- In some applications, imperfect security may be sufficient
- Need to analyse attack probabilities and economic impacts
- These factors can be taken in account in protocol design
- Our approach is to try *1. understand the potential mechanisms for weak authentication*, *2. categorize them*, and *3. build models for their analysis*

Weak Authentication Toolbox

- Spatial separation
  - Ensure peer is reachable via a specific communications path
  - Physical contact / network path / quality of path
  - Single path / multiple paths
- Temporal separation
  - Ensure peer is still the same peer
  - Session / Inter-Session
- Asymmetric cost wars
  - Scanning cost / attack cost / cost of revealing location
- Application semantics
  - Cryptographic semantics of identifiers
- Transitive and combined methods

Toolbox Dimensions



Weak Authentication Methods (1/2)

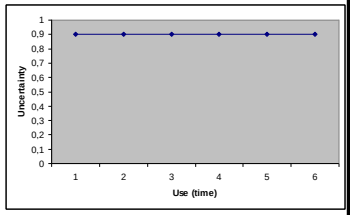
- Challenge-Response (CR) – Spatial
  - E.g. SIP null authentication or Mobile IPv6 Return Routability
  - Does node X receive packets sent to address A?
- Anonymous Encryption (AE) – Temporal, Cost
  - Unauthenticated Diffie-Hellman
  - The remainder of the session is encrypted and integrity protected

Weak Authentication Methods (2/2)

- Leap of Faith (LoF) – Temporal, Spatial, Cost
  - At first usage, an unauthenticated key agreement
  - Subsequent connections authenticated using these keys
  - E.g. SSH, HIP
- Cryptographically Generated Addresses – Spatial, Application
  - Part of an address is a hash of a public key
  - *IPv6 Address = <routing prefix> | hash(PK)*
  - Private key can be used to prove I am the "owner" of the particular IPv6 Address

Anonymous Encryption (AE)

- Defeats passive attacks
- Uncertainty depends only on the probability of a MitM on the link



Economic Analysis of AE

- The previous analysis considers only an individual - what if everyone used AE?
- Economic assumptions:
  - Cost of scanning $ 0.1
  - Cost of eavesdrop $ 1.0
  - Cost of MitM $ 10.0
  - One “interesting” person per million

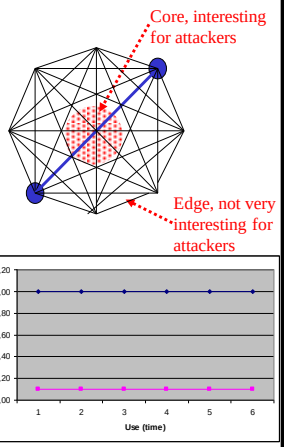
AE Individual Use vs. Global Use

	Scanning	Other	Total
No AE	$100 000	$1	$100 001
AE for the interesting person	$100 000	$11	$100 011
AE for everyone	$10 000 000	$1	$10 000 001

- Conclusion: while not useful for a single individual, techniques like this can raise the costs for an attacker, on a global scale
- Depends on the assumptions -- if the attacker doesn’t care who to attack the result is very different

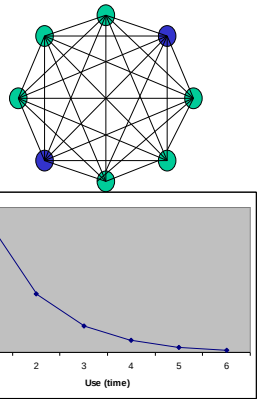
Challenge-Response

- Factors:
  - Spatial separation & ability to see challenge
  - Freshness
- Simple model:
  - P(MitM on a specific path) = 0.1
  - Number of paths = N
  - No challenges =>
    P(attacker on some path) ~ 1
  - Challenges =>
    P(MitM on a specific path) = 0.1



Leap of Faith

- Factors:
  - Temporal separation
  - Spatial separation
- Simple model:
  - P(a MitM on a specific link) = 0.9
  - Different MitMs N=2
  - 1. use =>
    P(attack) = 0.9
  - 2. use =>
    P(attack) = 0.9 * 1/2 = 0.45
  - k. use =>
    P(attack) = $P^k * (1/N)^k$
  - Note that if one link is known to be MitM free, then attacks no more possible



Conclusions

- In some application, imperfect security is good enough
- Uncertainties related to Weak Authentication and economic impacts for attackers can be surprising
- Understand the above in the context of the application, and then design protocols