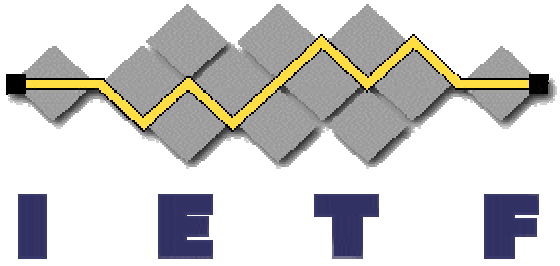
IETF Security Overview

Russ Housley
IETF Security Area Director
housley@vigilsec.com



2 May 2005

Outline

- Introduction
- Security Services and Mechanisms
- Security Protocols

The Internet Environment

- The Internet evolved in a world without predators; denial-of-service was viewed as illogical and undamaging
- The world today is hostile, and a tiny fraction of the machine population can do a lot of damage
- The Internet connects mutually distrustful organizations and individuals without central management
- Society expects a reliable Internet, which exceeds “traditional” security concerns

Security is …

- Data is only disclosed to intended recipients
- Monitor and track down “bad guys”
- Prevent data corruption
- Destroy computers with pirated content
- Anonymous communication

Security means different things
to different people!

Sometimes Security Goals Conflict

- Privacy vs. Company (or Government) desire to monitor network traffic
- Losing data vs. Disclosure
- Denial of service vs. Preventing intrusion

Intruders can …

- Eavesdrop
  - Links, compromise routers, routing algorithms, or DNS
- Send arbitrary messages
- Replay recorded messages
- Modify messages in transit
- Trick people into running malicious code

Email: Example to Motivate

- Send private messages
- Know the sender of the message
- Know the message has not been modified
- Non-repudiation – a third party can know the original sender and the message content
- Anonymity

Again, security means different things to different people!

Security Services (1 of 2)

- **Confidentiality**

  Assurance that the message content can only be read by the intended recipients

- **Data Integrity**

  Assurance that message content has not been altered

- **Authentication**

  Assurance that stated message originator is correct

- **Non-repudiation**

  Assurance that the original message originator cannot deny the message content

Security Services (2 of 2)

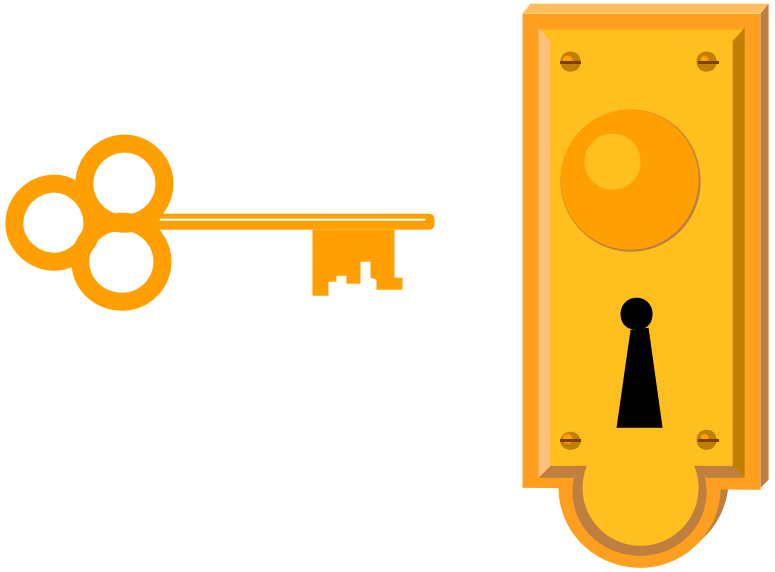
- **Access Control**

  Assurance that a resource can only be used in an authorized manner

  - Identity-based Access Control
  - Rule-based Access Control
  - Role-based Access Control
  - Rank-based Access Control

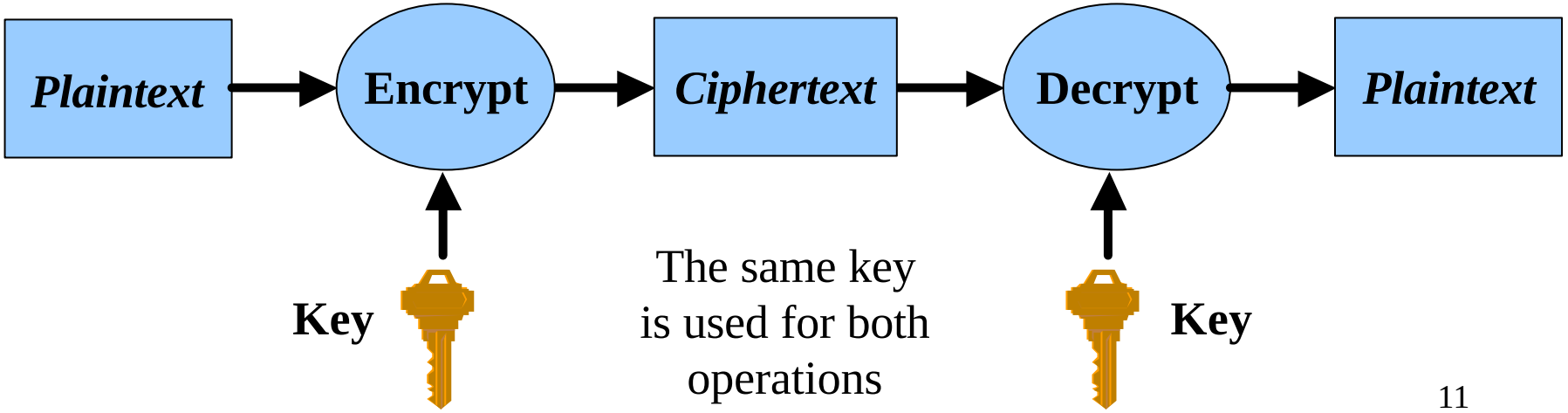
Confidentiality

- Encryption protects information from unauthorized disclosure
- Only parties that have the cryptographic key can recover the message content



Encryption

- Encryption renders a plaintext message unintelligible by all parties, except those that have the key needed to turn the ciphertext back into plaintext



Data Integrity

- Assurance that the message content has not been altered
- Cryptographic checksums, usually based on one-way hash functions, provide data integrity
- “Hashing” produces a small value that uniquely represents the message content
  - If two message contents differ only by a single bit, they will have very different hash values

One-way Hash Functions

- One-way hash functions provide data integrity
- Provide a hash value of uniform size for any length message
- Computationally infeasible to:
  - Derive the original message from the hash value
  - Create a second message with the same hash value as the original message

Authentication

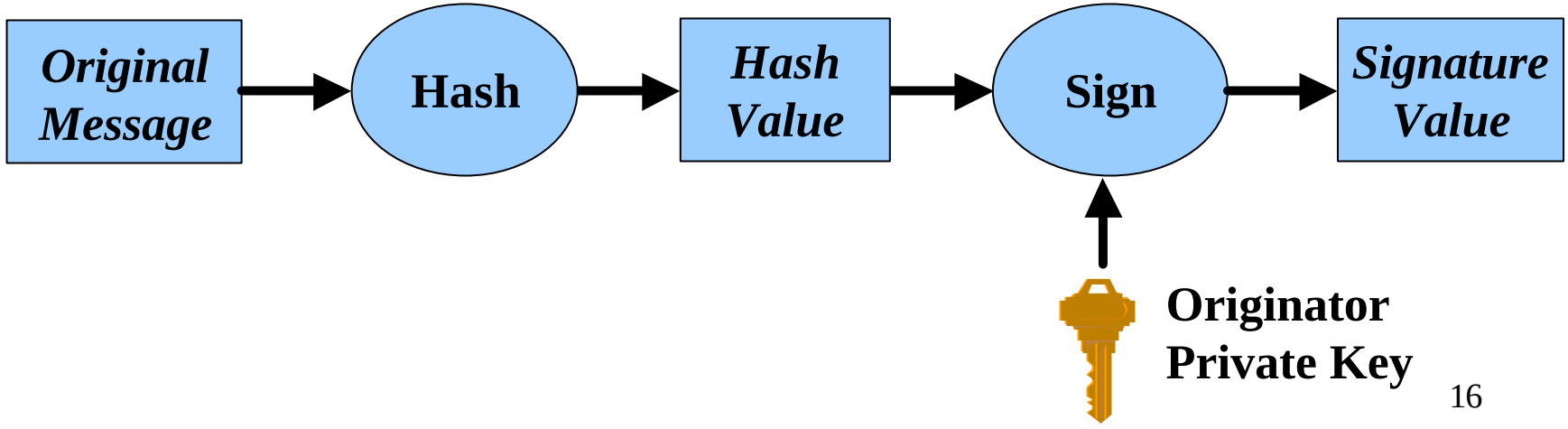
- Assurance that originator is as claimed
- Some authentication mechanisms can only be verified by a partner that shares a secret value, but others can be verified by anyone
- Today, we can do better than passwords …
- Authentication types:
  - Unilateral: server knows client
  - Mutual: peers know each other

Non-repudiation

- Assurance that the message originator cannot deny the message content
- A third party (like a judge or arbitrator) can verify the data integrity and authentication, preventing the message originator from falsely denying that they sent the message or it’s content
- Non-repudiation usually makes use of a digital signature

Digital Signature

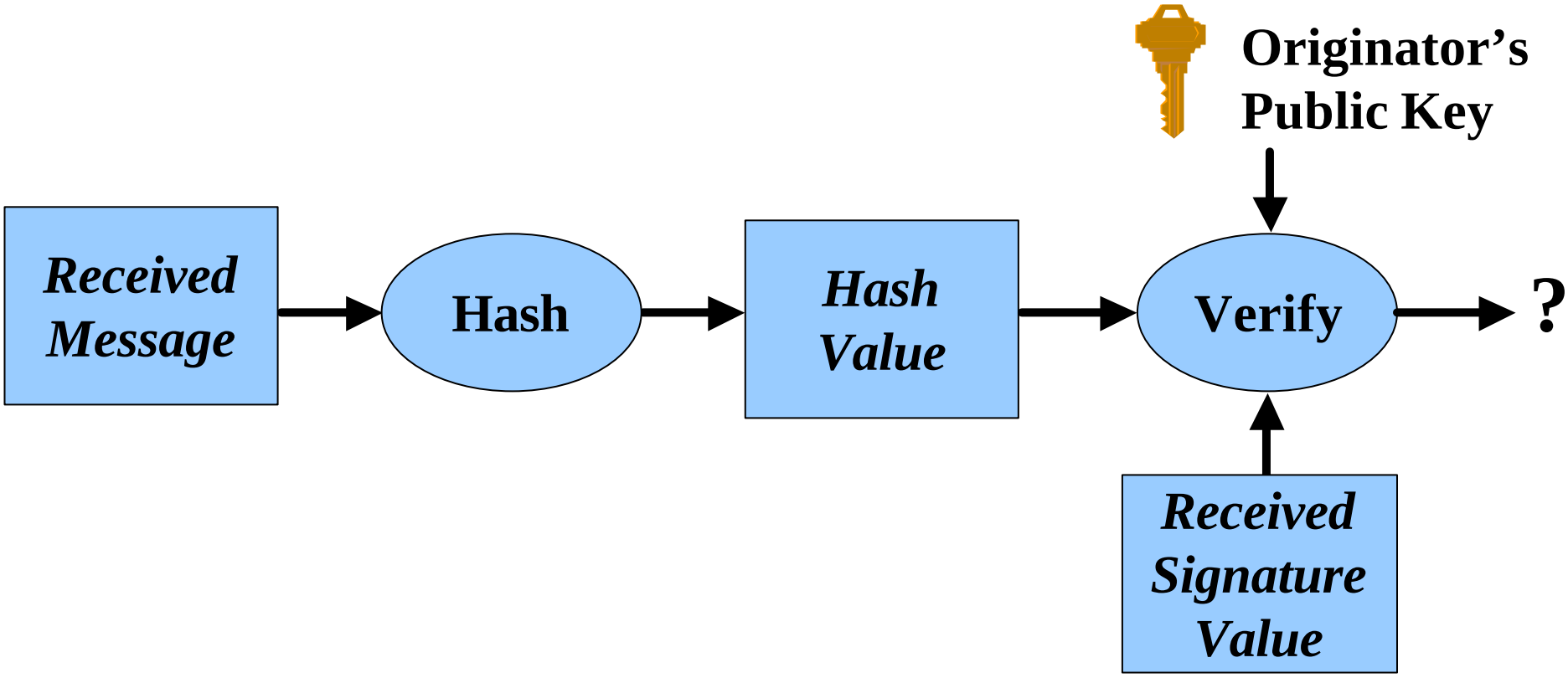
- A one-way hash function is used to create a hash of the data to be signed
- A digital signature is cryptographic transformation of the hash value and the signer's *private* key



Digital Signature Validation (1 of 2)

- The digitally signed message content and the digital signature value are sent to the recipient
- The recipient hashes the message content, then using the sender's *public* key, performs a digital signature verification
  - The recipient must not use the hash value computed by the message originator
- The verification will either pass or fail

Digital Signature Validation (2 of 2)



Security Protocols – Which Layer?

- Layer 2
  - Protects link hop-by-hop
  - IP headers can be hidden from eavesdropper
    - Protects against traffic analysis
- Layer 3 and Layer 4
  - Protects end-to-end real-time conversation
- Application Layer (e.g., S/MIME)
  - Protects messages
  - Supports store-and-forward communication

“Key Exchange”

- Mutual authentication/session key creation
  - Create a “security association”
- Prefer to cryptographically protect entire session, not just initial authentication
- Prefer a new key for each session
- Examples:
  - SSL/TLS or Secure Shell (Layer 4)
  - IKEv2 security associations for IPsec (Layer 3)

Layer 3 vs. Layer 4 (1 of 2)

- Layer 3
  - Do not change applications or their APIs
  - OS provides security protocol
- Layer 4
  - Do not change OS
  - Application program provides security protocol
    - Perhaps by linking with a library
  - Run on top of Layer 4 (TCP or UDP)

Layer 3 vs. Layer 4 (2 of 2)

- Layer 3 protects more of the protocol stack
  - Rogue packet problem
    - IPsec detects bogus packet injected by attacker before they are provided to TCP, which has no way to recover
  - Accommodates outboard hardware processing since each packet is independent
- Layer 4 is a lot easier to deploy
- Unless current API changes, layer 3 cannot provide authenticated identity to applications

Lesson learned:

Ease of deployment is more important than the robustness of the security solution

IETF Security Protocols

- S/MIME
- OpenPGP
- TLS (and DTLS)
- SRTP
- Secure Shell
- IPsec (including IKE, ESP, and AH)
- EAP
- Kerberos
- DNSSEC

Are more security protocols needed?

- Maybe; specific communications environments may require custom solutions.
- The bigger challenge is the integration of the existing security protocols with existing and emerging applications.

Invitation

While the IETF is not here to endorse or critique NGN, the IETF Security Area does:

- Support any technology that makes use of the existing security protocols
- Want to understand requirements for improvement of these security protocols for NGN or *any other technology*
- Want to understand these technologies to ensure the core IP network is not harmed

Please join us in the IETF to make NGN requirements for improvement clear, then work with us to provide solutions

Thank You

Russ Housley
+1 703-435-1775 (voice)
+1 703-435-1274 (fax)
housley@vigilsec.com