Introduction to Security Protocols

APNIC Open Policy Meeting
22 February 2005
Kyoto, Japan

Vigil
Security
LLC

Russ Housley
housley@vigilsec.com

Outline

- Introduction
- Security Services and Mechanisms
- Public Key Certificates
- Security Protocols

The Problem

- 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
- Must connect mutually distrustful organizations and people with no 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!

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

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

Examples to Motivate (1 of 3)

- File Sharing
  - File store must authenticate users
  - File store must know who is authorized to read and/or update the files
  - Information must be protected from disclosure and modification in transit
  - Users must authenticate the file store
    - Otherwise, files are given to the attacker

Examples to Motivate (2 of 3)

- Electronic Mail
  - 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

Examples to Motivate (3 of 3)

- Electronic Commerce
  - Pay for things without giving away my credit card number to an eavesdropper or phoney merchant
  - Buy anonymously
  - Merchant can prove who placed the order

The examples further illustrate:

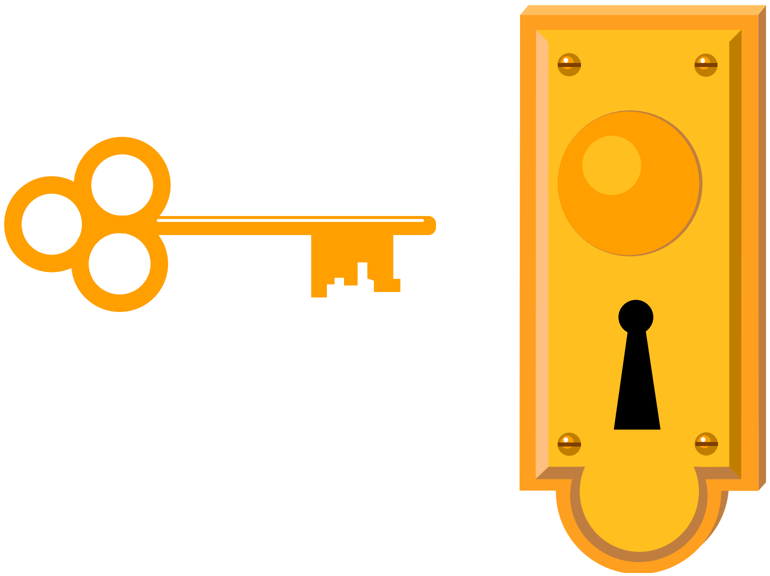
Security means different things to different people

Sometimes the goals conflict

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

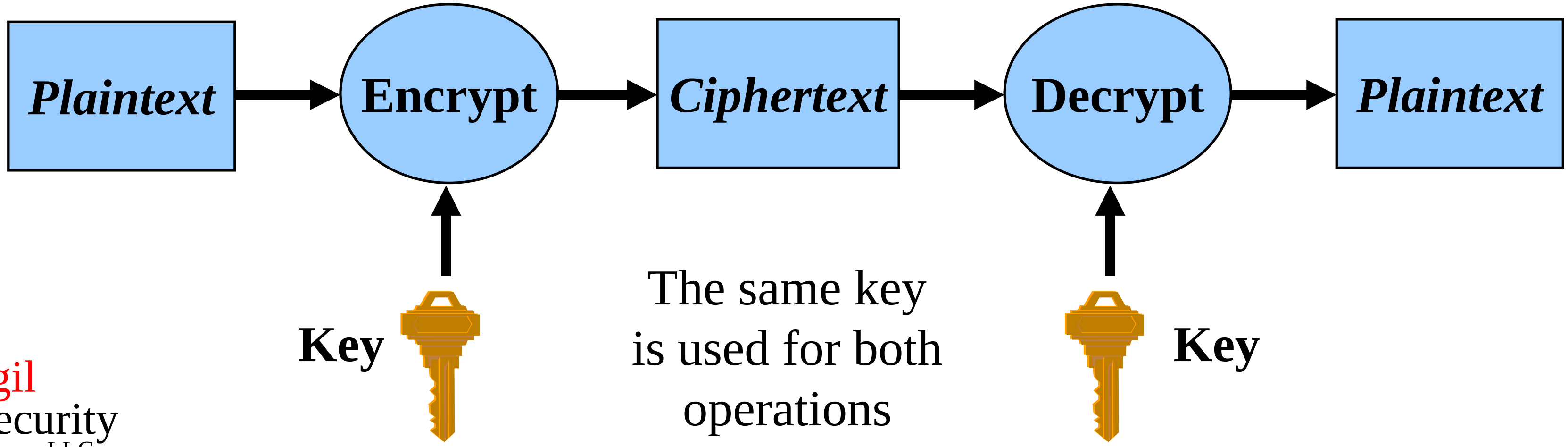
Confidentiality

- 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



Vigil Security LLC

Encryption Algorithms

- AES (Advanced Encryption Standard)
  - FIPS 197
  - Three key sizes: 128, 192, and 256 bits
- Triple-DES
  - ANSI X9.52
  - Either two or three 56-bit DES keys
- RC4
  - RSA Security
  - Variable length key, up to 256 bits

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

Vigil Security LLC

One-way Hash Functions (1 of 2)

- 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

One-way Hash Functions (2 of 2)

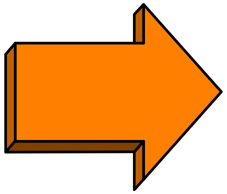
- SHA-1 (Secure Hash Algorithm 1)
  - FIPS 186-1
  - 160-bit hash value
- MD5
  - RSA Security
  - 128-bit hash value
- SHA-224, SHA-256, SHA-384, and SHA-512
  - FIPS 186-2 (and supplement)
  - 224-, 256-, 384-, and 512-bit hash values

Authentication

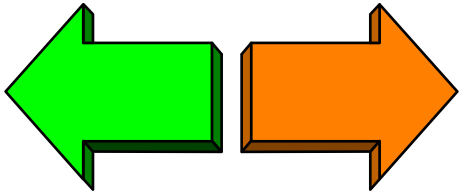
- Assurance that message originator is as claimed
- Some authentication mechanisms can only be verified by a partner that shares a secret value, but others can be verified by anyone
- Historically, authentication in computer and network systems is based on a user name and a password; however, more secure mechanisms
  are readily available

Unilateral and Mutual Authentication

- Unilateral (one-way)
  - User is authenticated to system



- Mutual (two-way)
  - User is authenticated to system
  - System is also authenticated to user



Non-repudiation

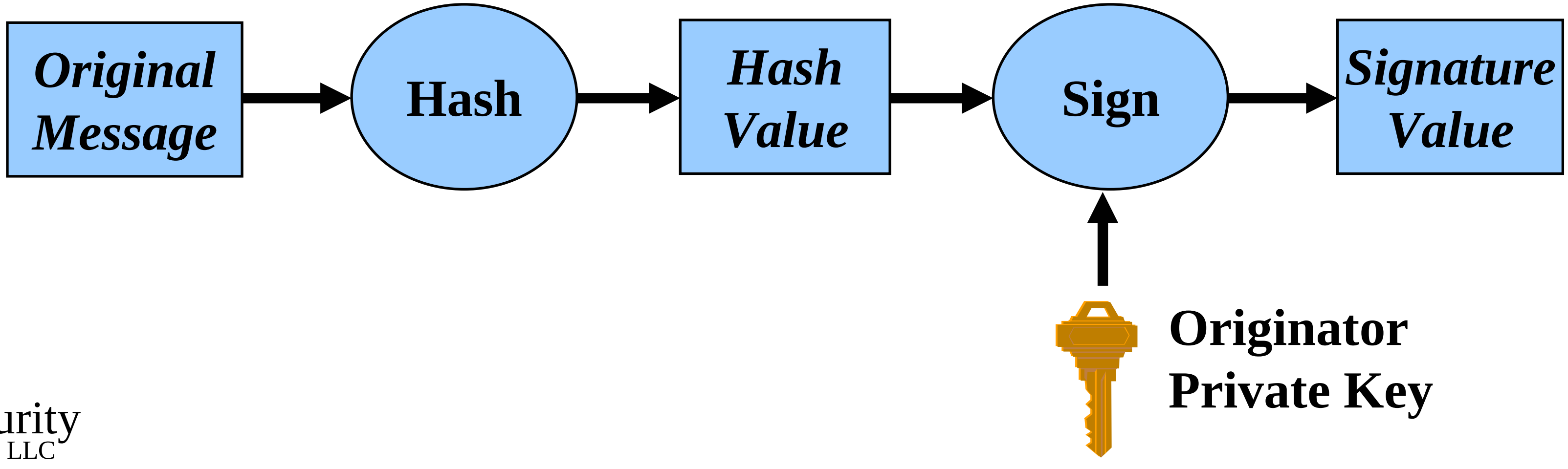
- Assurance that the message originator cannot deny the message content
- A third party (like a judge or arbitrator) can verify the data integrity and authentication, preventing the message originator from falsely denying that they sent the message or it's content
- Non-repudiation usually makes use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

Public Key Cryptography

- Public key cryptography is an important mechanism used to implement all of the security services
- Public key cryptography is often combined with other mechanisms in a total solution
- Two keys: public key and private key
- Common public key algorithms include RSA, DSA, Diffie-Hellman, ECDSA, and ECDH

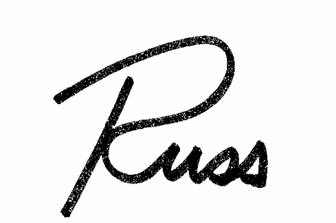
Digital Signature

- 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



Digitized vs. Digital Signature

- A digitized signature is a scanned image that can be placed on any document
- A digital Signature is a numeric value that is created by performing a cryptographic operation that involves the private key of the signer



Digitized Signature

1A56B29FF6310CD326109F200D5EF71
9A274C66821B09AC3857FD62301AA27
00AB3758B6FE93DE31009ACFCD39261

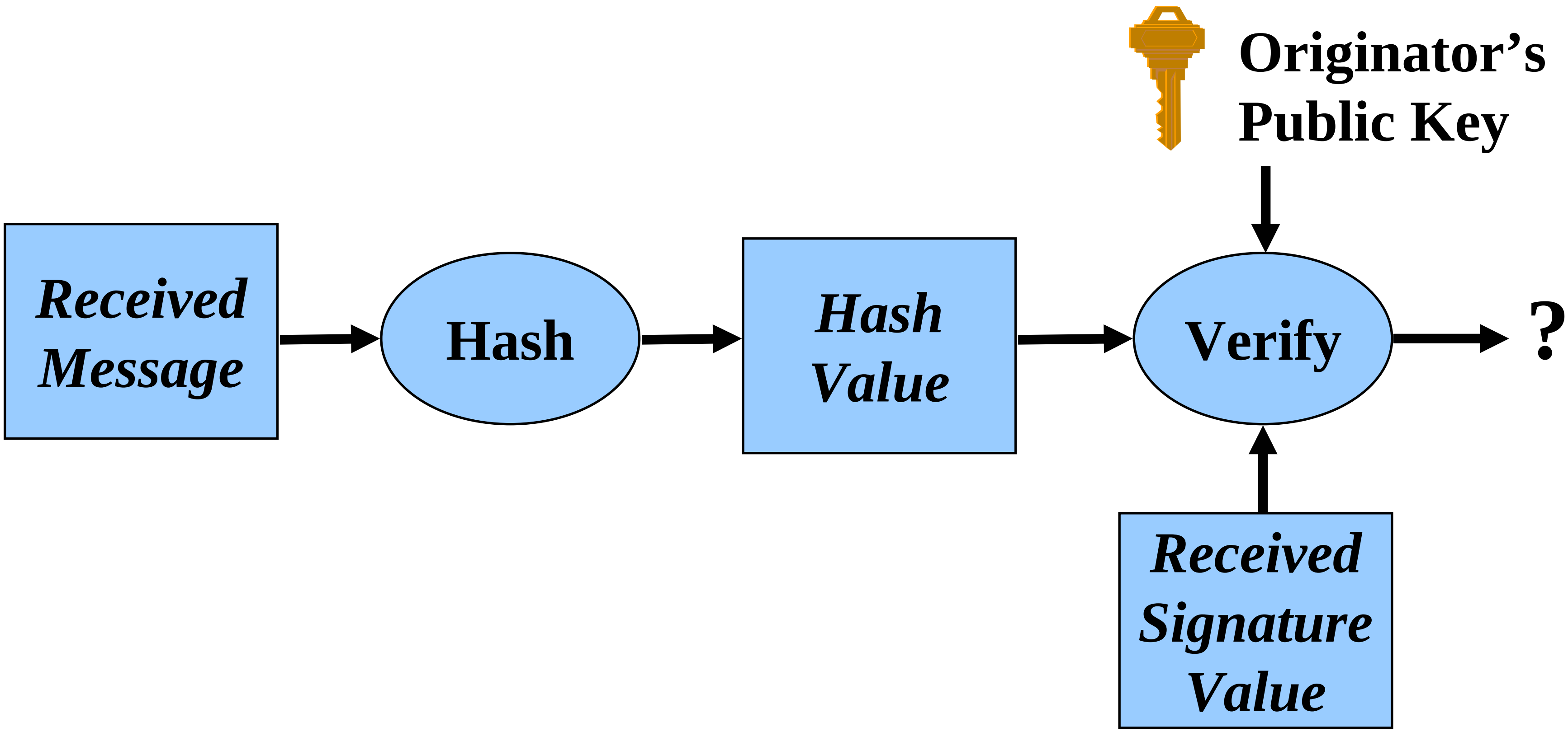
Digital Signature

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

Vigil Security LLC

Digital Signature Validation (2 of 2)



Digital Signature Algorithms

- RSA (Rivest-Shamir-Adleman)
- DSA (Digital Signature Algorithm)
- ECDSA (Elliptic Curve DSA)

Public Key Certificates

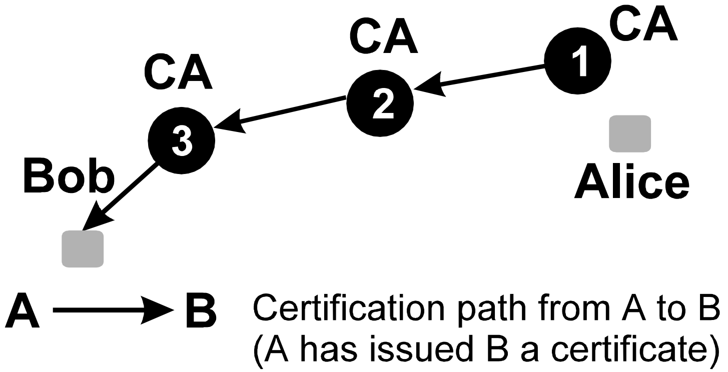
- Certificates bind an identity to a *public* key
- An issuing or certifying authority builds a certificate that contains:
  - Subject's Name
  - Subject's Public Key
  - Issuer's Name
- The issuer digitally signs the certificate
  - No one can change its contents

Certification Authority

- Establish and maintain an accurate binding between the public key and attributes contained in a certificate
- Manages and publishes certificates
  - Issues and renews certificate
  - Issues Certificate Revocation List (CRL)
- Initializes tokens (optional)
- Generates and provides recovery for public/private key pairs (optional)

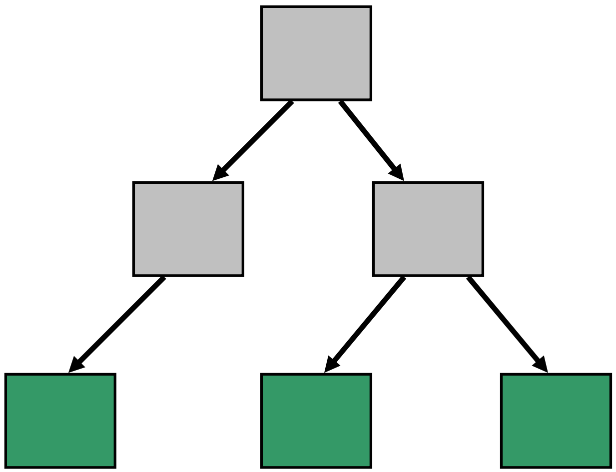
Certification Path

Alice can verify Bob's certificate by verifying a chain of certificates starting at one issued by a Certification Authority (CA) she trusts

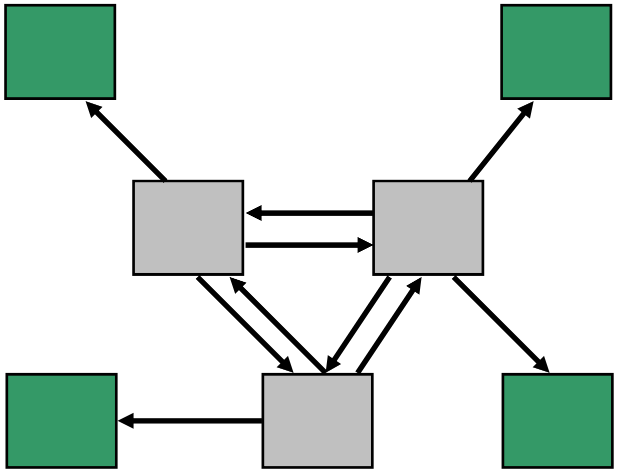


Public Key Infrastructure Topology

Hierarchy



Mesh

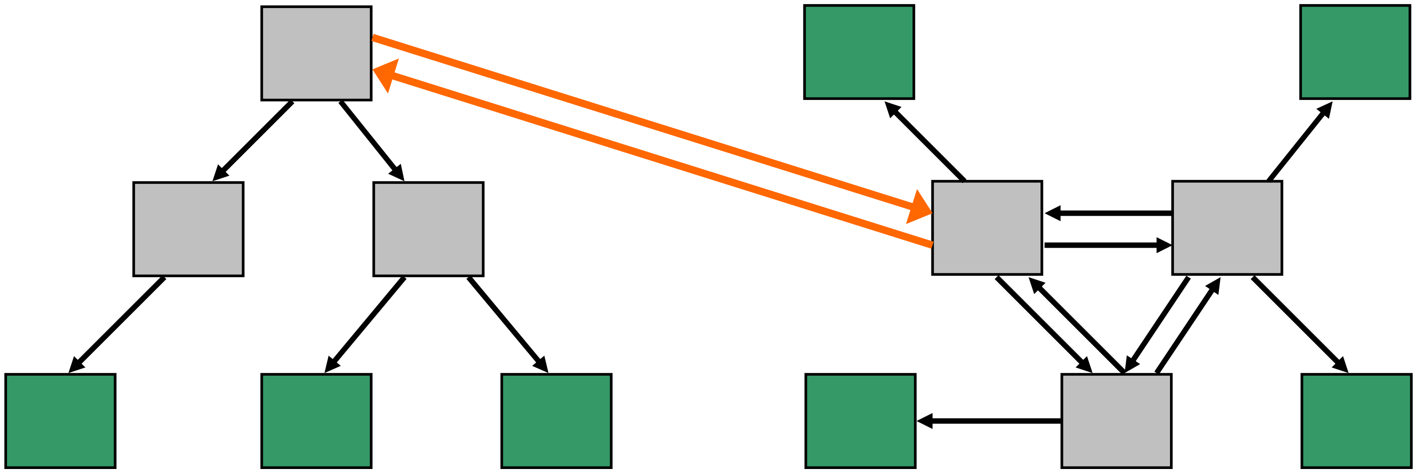


Vigil Security LLC

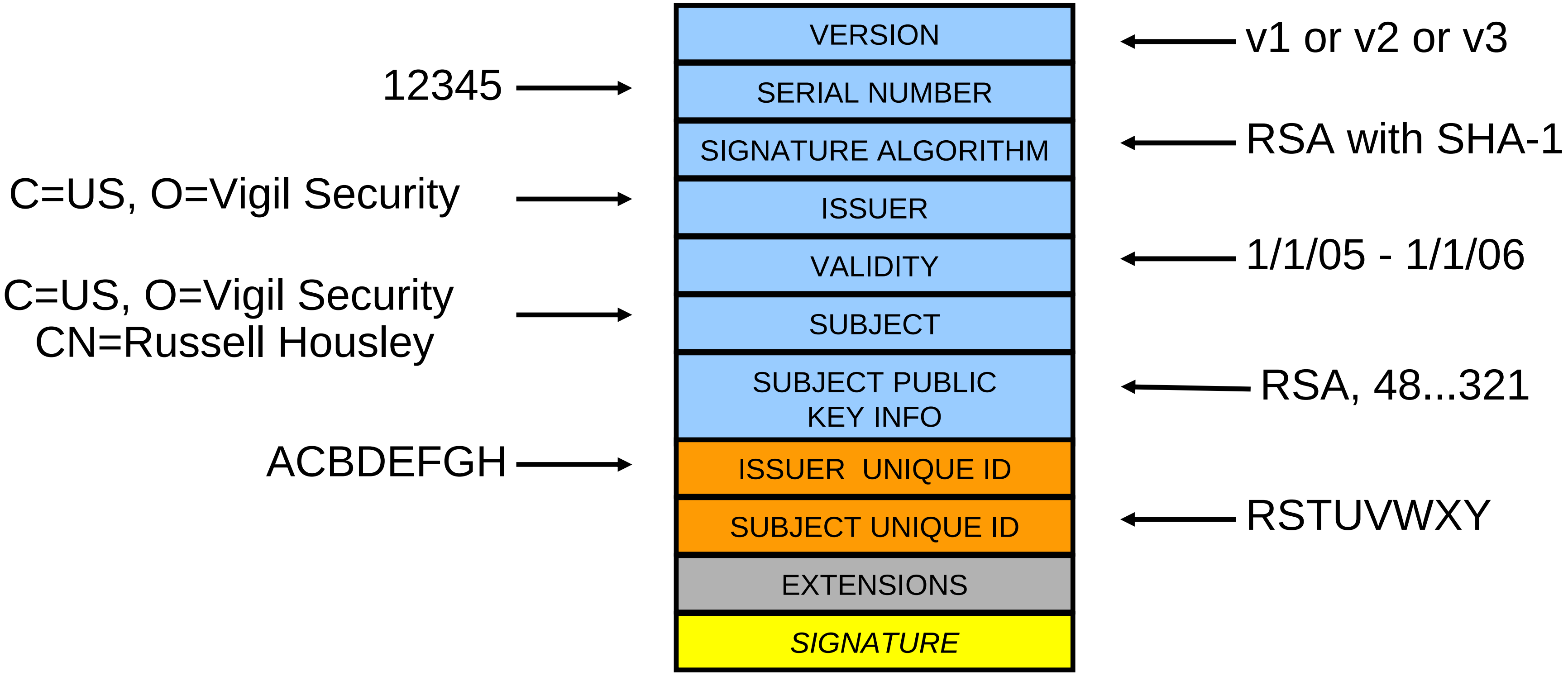
Which PKI Structure?

- Not a technology driven choice
- Choose the PKI Structure that best implements the organization’s policy
- A organization is authoritative for it’s members
- One *trust anchor* can support multiple certification policies and multiple public key algorithms

Cross Certification



X.509 Certificate Format



Vigil Security LLC

Name Forms

- Certificate subject and issuer identified by:
  - X.500 Distinguished Name
  - DNS Name
  - Internet E-mail Address
  - WWW URI
  - IP Address
  - Others . . .

X.509 Certificate Extensions

- Authority Key Identifier
- Subject Key Identifier
- Key Usage
- Private Key Usage Period
- Certificate Policies
- Policy Mappings
- Subject Alternative Name
- Issuer Alternative Name
- Inhibit Any-Policy
- Basic Constraints
- Name Constraints
- Policy Constraints
- Extended Key Usage
- CRL Distribution Points
- Subject Directory Attributes
- Authority Information Access
- Subject Information Access
- Freshest CRL

Attributes in Certificates

- Accurate binding of attributes to a public key
  - identity
  - authorization
  - policy expression
  - PKI management
- Is the CA authoritative for the attributes in the certificate?
- Steve Kent's Rule of Revocation:

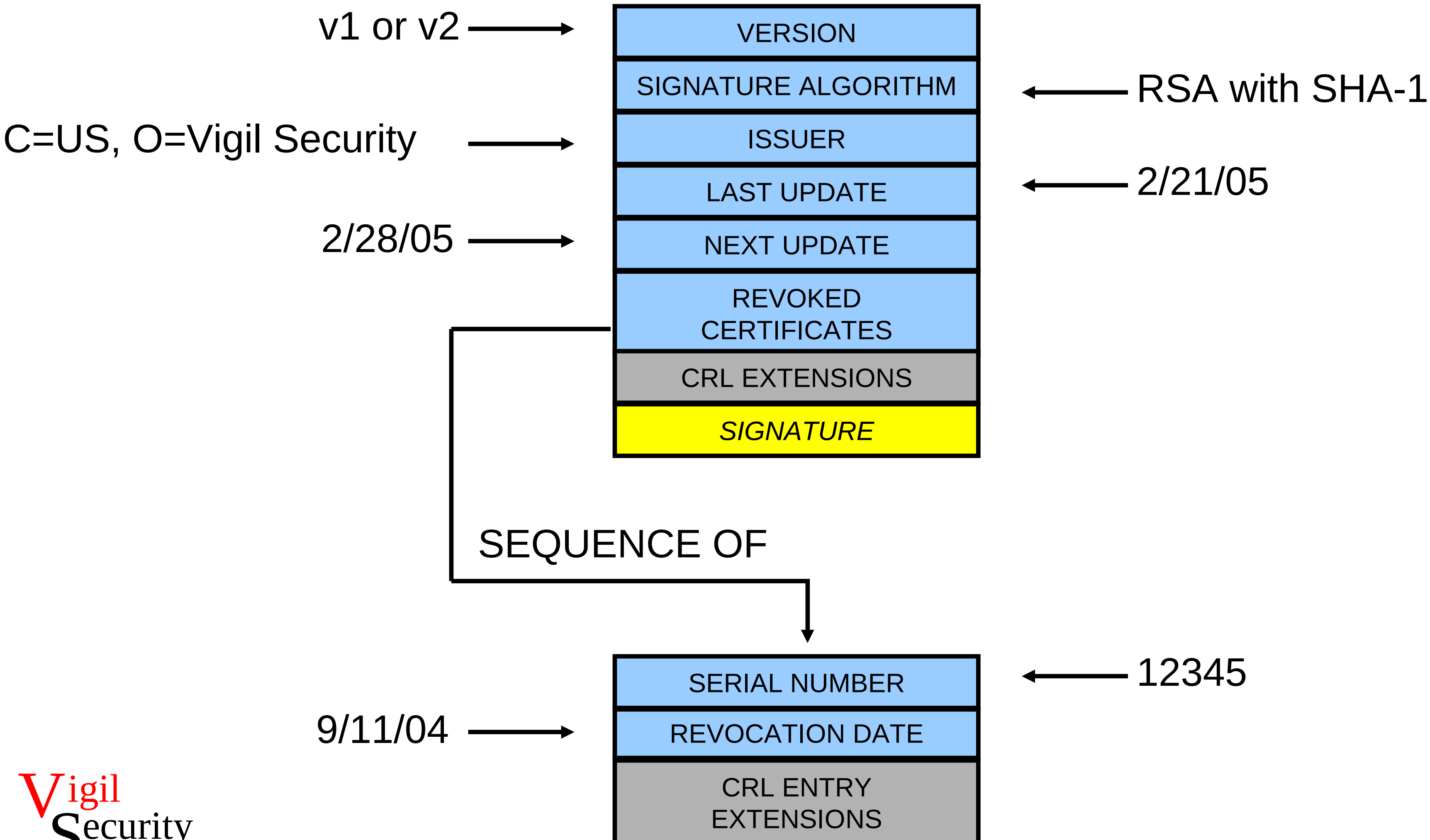
  " The effective lifetime of a certificate is inversely proportional to the square of the number of attributes. "

Vigil Security LLC

But, Things Change …

- Who owns the private key?
  - Certificate binds the private key owner's identity to the public key
- Is this binding still valid?
  - Certificate Revocation List (CRL) provides a list of the unexpired certificates that should no longer be used
    - Private key compromise
    - CA compromise
    - Affiliation changed
    - Superseded
    - CA ceased operation
    - …

X.509 CRL Format



Vigil Security LLC

Trust in Certification Authorities

- CA trust should not be binary
  - "Is this CA trusted?"
- Instead, a CA should only be trusted for certain certificates
  - "Can I trust this CA to issue certificates for secure electronic mail?"

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 “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)
  - 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 technically superior
  - Rogue packet problem
    - IPsec detects bogus packet injected by attacker before they are provided to TCP, which has no way to recover
  - Accommodates to do 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

IPsec ESP

SPI identifies security association

SEQUENCE NUMBER detects replayed packets

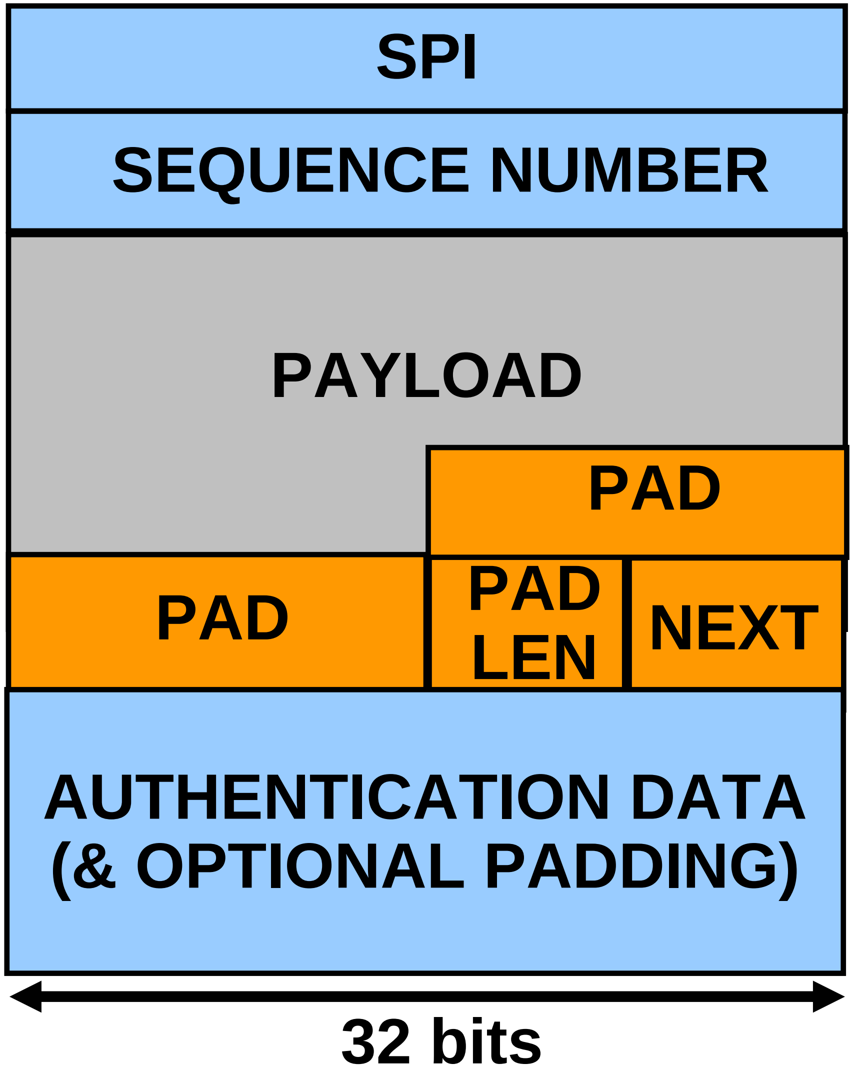
PAYLOAD protected data, prefixed by an IV if required

PAD extends the plaintext payload

PAD LEN indicates the pad length

NEXT identifies payload protocol

AUTHENTICATION DATA contains integrity check value



Vigil Security LLC

Lesson learned:

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

Vigil Security LLC

Questions?

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