The Trouble With Standard Protocols

Dr. Robert W. Baldwin
Plus Five Consulting, Inc.

The Trouble

- “Let them Eat Cake” – Marie Antoinette
- “Let them Use Standards” – Anonymous

Outline

- “THE” Standard Protocols
- Constraints of New Markets
- Engineering Tricks

The Standard Protocols

Protocol	**Type**	**Extra Msgs**	**Extra Data**	**RSA Ops**
SSL	Point-to-Point Interactive. 1 or 2-way Authentication.	3 TCP + 3 or + 6	2 KB +2 KB	2 Pub. 1 Priv. [1 Pub]
S/MIME	One-way. Multicast. Sign / Encrypt.	N/A	2 KB	1 Pub. 1 Priv.

Protocol Assumptions

Protocol	**Channel Bandwidth**	**Channel Latency**	**Channel Attacks**
SSL	Medium to High. Cheap.	Low connect. Low packet.	Active Easy.
S/MIME	Medium to High. Cheap.	High OK.	Active Easy.

Protocol Assumptions

Protocol	**CPU Power**	**RAM & ROM**	**Disk & Cache**
SSL	Medium (never high)	Megabytes	Server:Big Client:Small
S/MIME	Medium	Megabytes	Both Medium

Protocol Assumptions

Protocol	**Trust Symmetry**	**Trust Duration**	**Motivation Re: Content**
SSL	Stranger to Brand Name. Trusted Root.	One Session.	Client & Server Honest.
S/MIME	Stranger to Stranger. Trusted Root.	One Message.	Everyone Cheats.

Outline

- “THE” Standard Protocols
- Constraints of New Markets
- Engineering Tricks

New Communication Channels

- Battery Powered Devices
- Two-Way Pager
- Local Infrared and Local Wireless
- High Bandwidth RF
- Shared Channel Cable Modem
- Point to Point Fiber Optic

New Computing Devices

- Electronic Lock, Remote Sensor, RF Tag
- MP3 Player (DSP & custom VLSI)
- Handheld (IR)
- Network Game Station, Set Top
- Integrated Phone/Browser/E-Mail/PDA
- Integrated Pager/E-Mail/PDA
- Secure Telephone, Videophone, Fax, Printer

“New” Trust Models

- Subscriber & Publisher
  - Cable TV, eBooks, Stock Reports
- Employee & Employer
  - Intra-Office Mail, Online Calendaring, Stock Trading, Order Entry,
  - Remote Sensing and Control.
- Mercantile Exchange
  - Inter-Company E-Mail. Customer Order Tracking. Trusted MP3 Player. EDI Exchange.

Outline

- “THE” Standard Protocols
- Constraints of New Markets
- Engineering Tricks

Avoiding Protocol Flaws

- Start with Standard Protocol
- Apply Security-Neutral Improvements
- Check Inter-Layer Assumptions
- Check Crypto-Primitive Assumptions

Reducing Extra Messages

- Integrate Layers or Phases of Protocol.
- Ex: TCP and SSL Handshakes
  - Can build SSL on UDP instead of TCP.
  - Can use TCP Nonce as SSL Challenge.
- Ex: SSL Handshake & First Data Packets
  - Can skip SSL Finish Message.
    First Data Message proves handshake worked.

Reducing Extra Data

- Assume Peer Knows Certificate Chain. Cache Certs. Track What Peer Knows.
- Send Data inside RSA Signature or Envelope (use OAEP).
- Put Signing and Enveloping Keys in Single Certificate.

Reducing Extra Data

- Assume Fixed Set of Algorithms and Parameters. Avoid Negotiation.
- Use One Version Field to Describe Format of Entire Message.
- Use Fixed Length Values When Possible to Avoid Sending Length Fields.
- Use One Field for All Flag Bits.

Reducing CPU Demand

- Avoid RSA Private Key operations
  - Keep Public & Private keys Secret.
    Client Signs with Secret Public Key.
- Remember RSA Results for Months.
- Avoid All RSA Operations
  - Triple-DES Key Distribution Center and
    Put Secret Keys in Clients.

Reducing CPU Demand

- Alternatives Public Key Algorithms
  - Elliptic Curve (s/w: Odd, h/w: Even)
  - NTRU (big keys, easy math)
- Hash Message Authentication Code (HMAC) Instead of Public Key Signature
- Cipher Mode with Checksum (CBCC), or ANSI DMAC.

Reducing Code Size

- Small Number of Fixed Format Packets.
  - Reduce Parsing Code & Special Cases.
- Small Number of Crypto Constructs.
  - One Encrypt & Checksum.
  - One Public Key (Sign Inside Enveloped).
- Use Block Cipher for Encrypt, MAC, Hash, PRNG, Authentication.

Outline

- “THE” Standard Protocols
- Constraints of New Markets
- Engineering Tricks

Avoiding Security Nightmares

- “Only a Fool Would Take a Ship Into Uncharted Waters.” – Captain Arab
- Use Standard Protocol If Possible

- Get Expert Review of Any Non-Standard Protocol
- Risks vs. Rewards