Java / ActiveX Security

David Gristwood
Senior Consultant
Microsoft Ltd

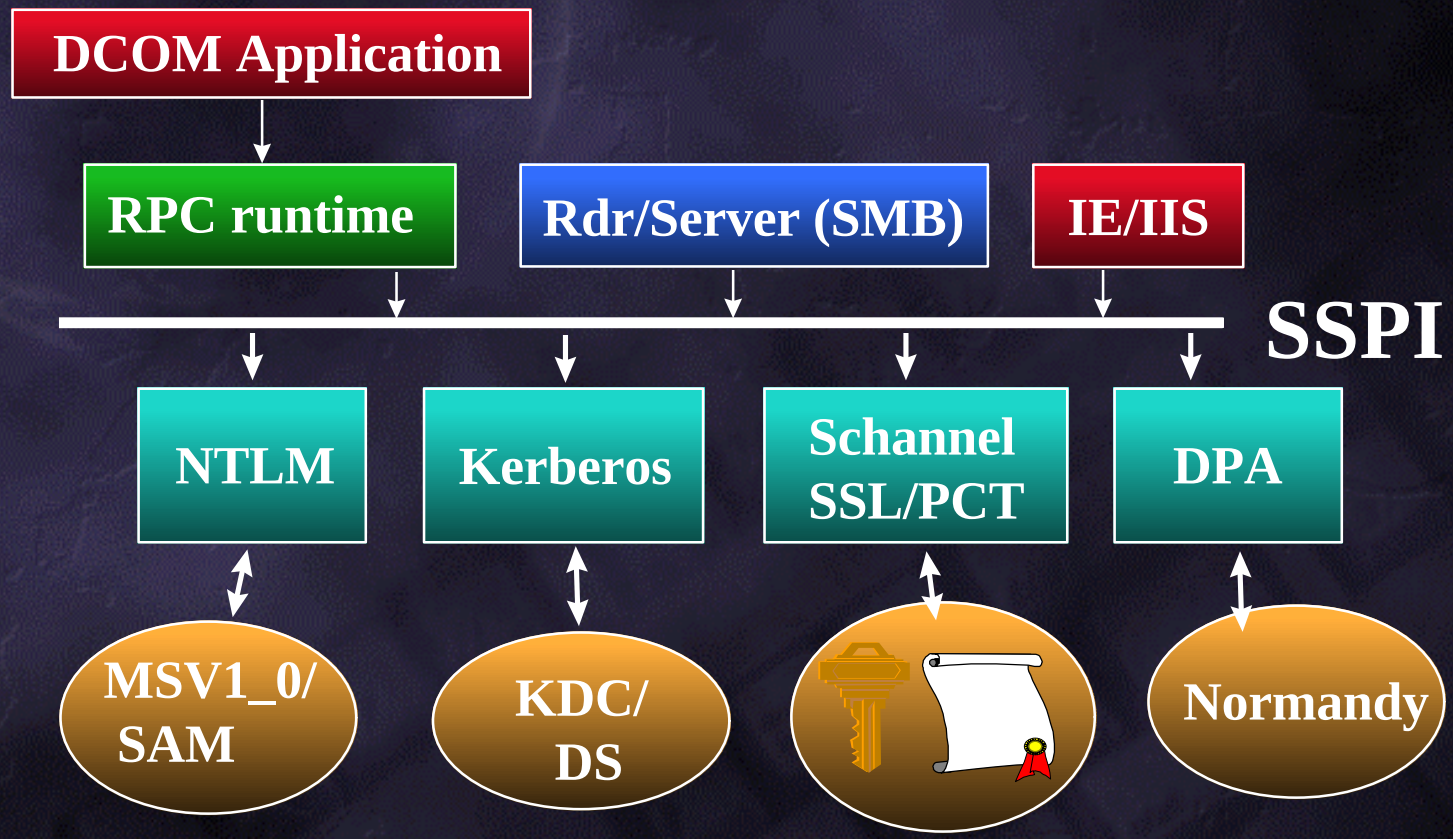
Security Issues

- Covers many areas:
  - Transact business securely
  - Ensure privacy of conversations
  - Authenticate users in communications
  - Ensure integrity of data
- Share much in common
  - Require security based infrastructure
  - Single solution cannot cover all aspects
- Not unique to the Internet - just magnified

Microsoft Internet Security Framework

Integrating Existing Security Models

Enabling Staged Migration to Public-Key Security



Public Key Components

For clients

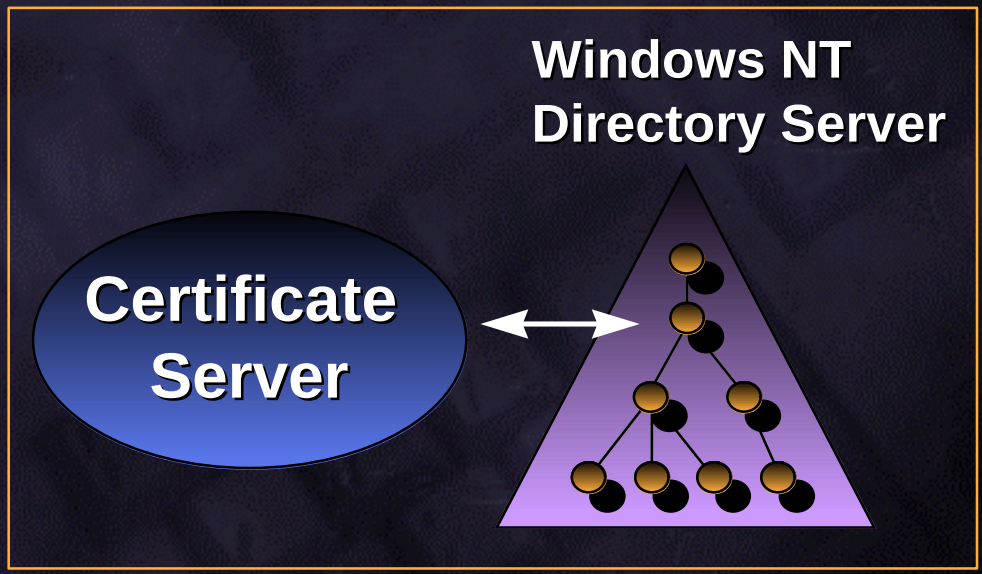
- User key and certificate mgmt
- Secure channel
- Secure storage
- CA enrollment

Enterprise

- Certificate services
- Trust policy

For servers

- Key and certificate management
- Secure channel
- Client authentication



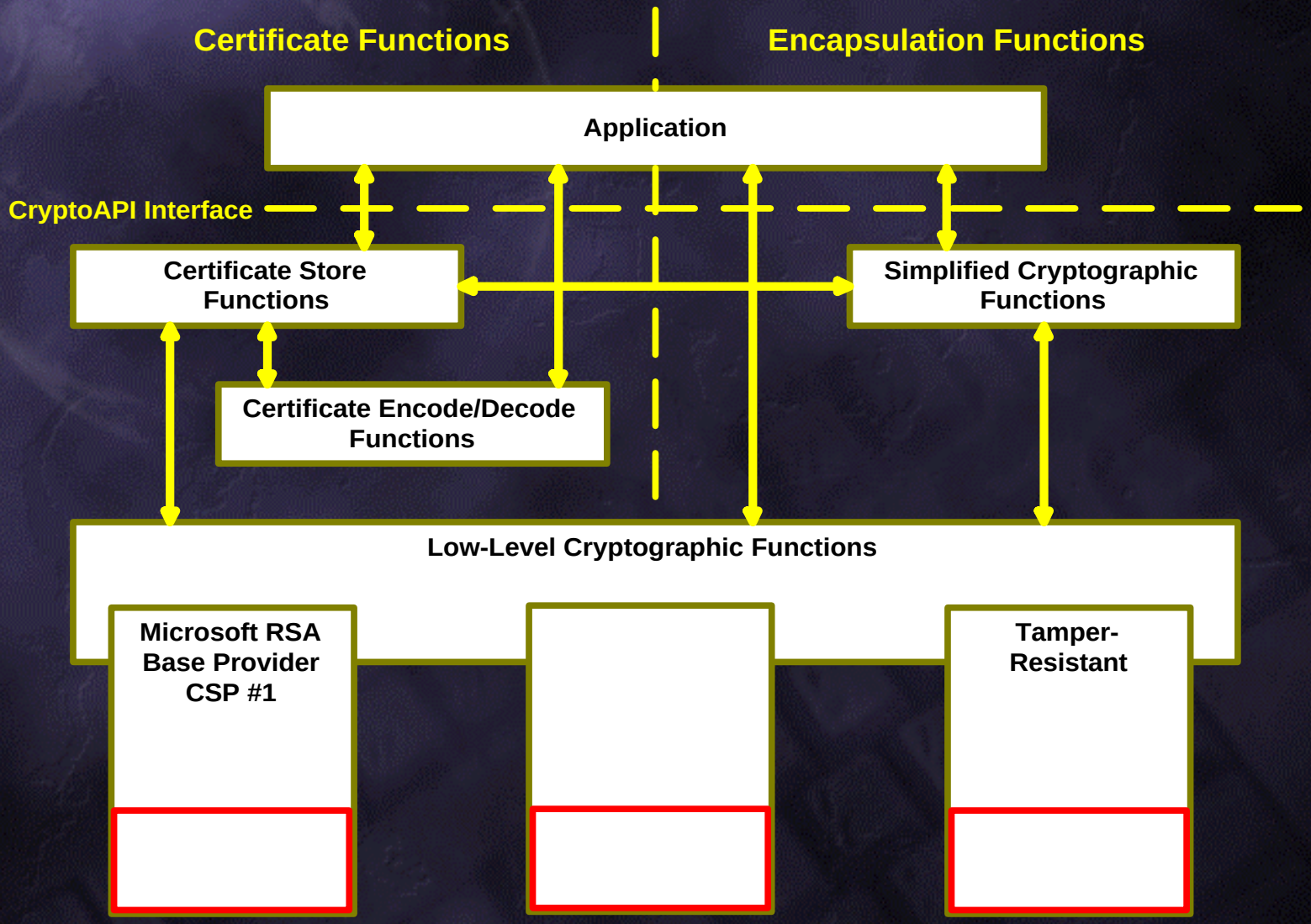
Crypto API

Foundation for public key security

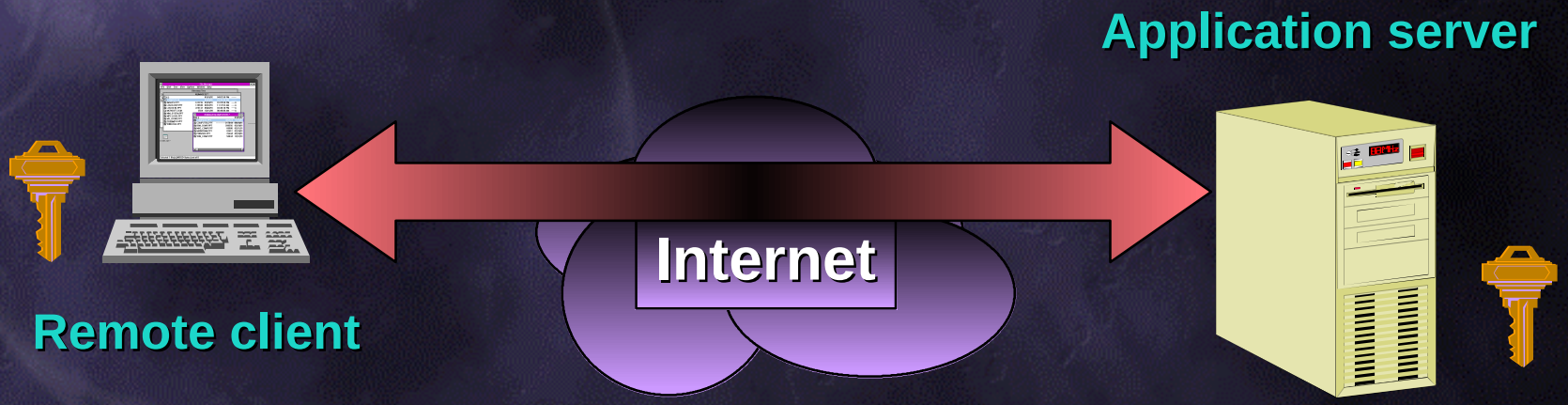
Internet Explorer 3.0, Windows NT 4.0

- Key generation and management
- Key exchange (RSA)
- Encryption/decryption (RC2 RC4)
- Hashing, signing, and verification (MD2 MD5 SHA)
- Service Provider model
- Encapsulation
  - E.g., PKCS #7
- Certificates
  - E.g., X.509 v3
  - Parse and verify
  - Storage mgmt

CryptoAPI 2.0 Architecture

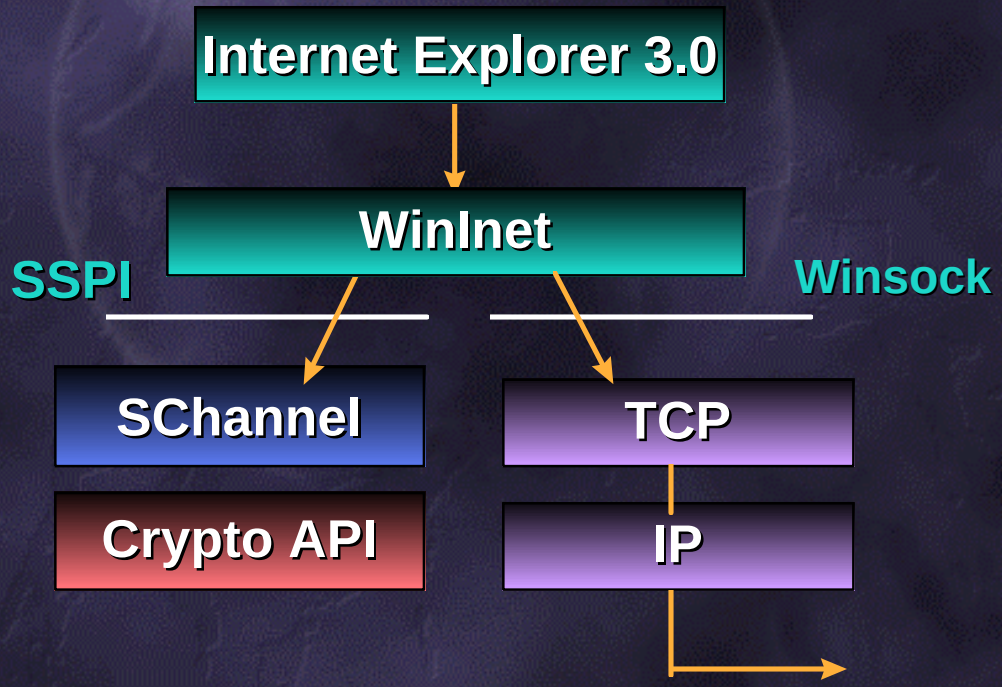


Secure Channel



- Secure channel provides:
  - Privacy: packets can't be snooped
  - Integrity: packets can't be altered
  - Authentication: no TCP/DNS spoofing
- Support for SSL2, SSL3, PCT1
  - IETF Transport Layer Security (TLS)

SChannel Architecture



- Application uses WinInet, requests SSL session
- WinInet uses SSPI and Winsock APIs
- SChannel SSP uses Crypto API for signatures

Microsoft Wallet

- Users own personal information; not an application or the system
  - Information is transportable (PFX)
  - Access policy defined by the user
- Microsoft Wallet:
  - Stores personal information including certificates, keys, passwords, credit card numbers, & more
  - Information kept secure based on access control policy
- Open, cross-platform, interoperable
  - Standards-based import, export, interchange to move information across platforms (MS PFX submission to a W3C initiative)
- Will ship in IE 4.0 and future versions of Windows

Microsoft® Certificate Server

- Manages the issuance, revocation, and renewal of public key certificates
- For organizations that want control over public key credentials
  - For specific applications or user identification
- Standards-based, transport-independent
  - X.509, PKCS, SSL/PCT, emerging IETF PKIX
- Complete control over certificate formats, extensions, and policies
- Integrates with Windows NT Directory Service using LDAP

Using the security framework

- Framework to build security around
  - Operating systems, networks, applications, management, etc.
- Strong support for distributed component based architectures
  - Desktop: Java™ applets, ActiveX™ controls, etc
  - Server: Microsoft Transaction Server components, Active Server Pages, etc

Point 1

- Microsoft supports Java™ and ActiveX™

Point 2

- This is not an either or contest
- It’s about trade-offs

Downloading Code to the desktop

Greater power = greater risk

- Current Web pages are informational and static, but changing to be active
- Risks include:
  - Malicious code
  - Tampered code
  - Unknown sites/authors
  - Impersonations
- Current Internet download behaviour not adequate for new paradigm

Java™

- If security is paramount, use Java
- Microsoft has Win32 reference platform
- Microsoft VM is the best way to run Java
  - Fastest - Microsoft wins the benchmarks
  - Most robust - Many complex Java apps can't run at all on other VMs
  - Most functional - debugging, JIT API, run Java apps standalone, native code and COM interfaces, ActiveX integration, faster applet downloads

The “Sandbox”

- “Sandbox” isolates applet in own Virtual Machine
  - Microsoft provides ActiveX™ Runtime for Java™ in Internet Explorer 3.0
  - VB Script is also a sandboxed language
- Effective, but not always sufficient
  - Requires provably secure interfaces, proven difficult in practice
  - Runs all code in sandbox with “least common denominator” capabilities
  - Some useful applications not possible

Complementary Solution: Digital Signatures

- Digital signing is industry-standard, established security solution
- Identifies and provides details about the publisher: publishing code on the Internet is no longer anonymous
- Validates the integrity of the image: guarantees that the image has not been altered from the time it was signed
- Analagous to “shrink-wrap” for Internet code
  - Approach validated by Sun®, JavaSoft, and Netscape code-signing announcements

Authenticode™

Enable shrinkwrap software for the Internet / Intranet

- Provide proof of origin by authenticating the source and integrity of code
- Provide trust by validating the relationship between user and software publisher
- Provide strong assurance using public key cryptography
- Provide accountability and legal or business recourse

Security Zones

- Manage security policies by dividing the Web into zones, each with separate security settings
  - e.g. Intranet, Trusted Extranet, General Internet and Untrusted
- Customise settings on a zone-by-zone basis
  - Java Applets, plug-ins, scripting, secure communications, content, privacy, etc.
- Certificate Management feature
  - administrators decide which signed code to allow

Authenticode 2.0

- Developed in conjunction with VeriSign
- Provides support for time stamping
  - confirming that the code was signed during the effective period of the publisher's certificate licence
- Online status and revocation checks
  - check before downloading


Microsoft®
where do you want to go today?
Start