



FY2001 ONR CIP/SW URI



Software Quality and Infrastructure Protection for Diffuse Computing



Principal Investigator: Andre Scedrov
Institution: University of Pennsylvania
URL: <http://www.cis.upenn.edu/spyce>

OPTION STARTED IN MAY 2004

The SPYCE Team



- Joan Feigenbaum (Yale)
- Joseph Y. Halpern (Cornell)
- Patrick D. Lincoln
- John C. Mitchell (Stanford)
- Andre Scedrov (U Penn)
- Jonathan M. Smith (U Penn)
(until December 2003)



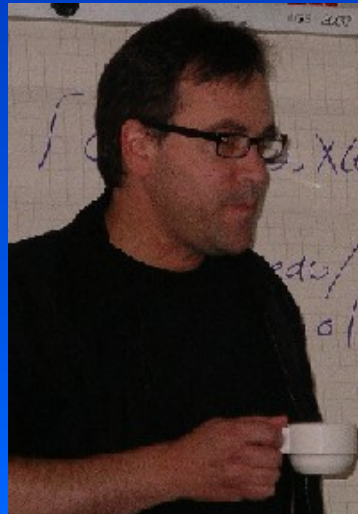
External Collaborators

Microsoft

Microsoft
Research

intel.

- Cynthia Dwork (Microsoft)
- Tim Griffin (U Cambridge)
- Vitaly Shmatikov (U Texas)
- Paul Syverson (NRL)



Postdocs

- Björn Knutsson, Penn (till Spring 2005)
- Ninghui Li, Stanford (until Summer 2003, now at Purdue Univ.)
- Michael Elkin, Yale (Fall 2003 - Summer 2004,
now at Ben Gurion Univ., Israel)
- Gergei Bana, Penn (Fall 2004 - Summer 2005)
- Anupam Datta, Stanford (starting in Fall 2005)

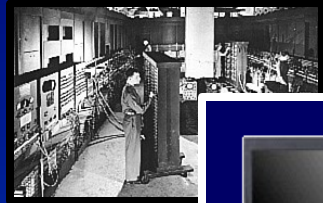
- 22 Ph.D. Students

Software Quality and Infrastructure Protection for Diffuse Computing

U Penn, Stanford, Cornell, Yale

URI, May 2001 **Email:** scedrov@math.upenn.edu **WWW:** <http://www.cis.upenn.edu/spyce/> Nov. 10, 2005

Smart devices diffuse into the environment....



Room '40s



Desktop '80s



Wearable '90s



Pervasive '00s

... with control and assurance

DoD Capabilities

Reduced cost, improved performance, and higher reliability for networked operations across untrusted networks

URI Objective

Algorithms to model, manage and maintain a computational infrastructure, distributed among many heterogeneous nodes that do not trust each other completely and may have incentives (needs, priorities).

Scientific/Technical Approaches

Computing and networking elements diffusing into the environment need:

- Local incentive-compatibility
- Scalable authorization mechanisms
- Assured communication
- Experimental evidence

Diffuse Computing

- Paradigm developing rapidly as a result of
 - commercial computing markets
 - now-recognized potential of *peer-to-peer* computing and *grid* computing
 - the need for distributed network-centric systems
- Raises challenges for
 - system design
 - software production
 - the development of mechanisms ensuring stable equilibria of diffuse systems

Breaking and Fixing Public-Key Kerberos

- Part of ongoing formal analysis of Kerberos 5 suite
 - Previously studied core part of protocol and cross-realm authentication
 - Focus on PKINIT, public-key extension to Kerberos
- Attack on PKINIT found when using “public-key mode” (one of two possible modes)
 - Breaks binding client’s request and the response
 - Prevents full authentication and confidentiality
- Formal verification of fixes preventing attack
 - Close, ongoing interactions with IETF Working Group
- Our work caused an August 2005 Microsoft security patch for Windows 2000, Windows XP, and Windows 2003
 - www.microsoft.com/technet/security/bulletin/MS05-042.mspx

Attack and Fixes (Overview)

- Protocol level attack on PKINIT-25
 - Not a problem with crypto or implementation
 - Kerberos server believes he is talking to the attacker
 - Client believes she is talking to the Kerberos server
 - Attacker knows the key shared by the client and Kerberos server
- Possible because the Kerberos server does not sign data identifying the client
 - Attacker constructs request based on client's request
 - Kerberos server signs data from client, sends in reply to attacker
 - Attacker forwards this to client after learning keys
 - Ran Canetti, consulted on details of spec., independently hypothesized the possibility of an "identity misbinding" attack
- PKINIT-27 is intended to defend against this attack
 - Kerberos server signs data derived from client's identity

Consequences of the Attack

- The attacker knows the keys C uses; she may:
 - Impersonate servers (in later rounds) to the client C
 - Monitor C 's communications with the end server
- Other notes
 - Attacker must be a legal user
 - C is authenticated to end server as attacker (not as C)
 - The second key generation mode (Diffie-Hellman) appears to avoid the attack
 - DH mode narrowly deployed
 - Still need to prove formally security for DH

Kerberos Review

- Protocol goals
 - Repeatedly authenticate a client to multiple servers
 - Does not guard against DOS attacks
- Kerberos 4 - 1989
- Kerberos 5
 - Specified in RFC 1510 (1993), RFC 4120 (2005)
 - Extensions under development in IETF WG
- A widely deployed protocol
 - Windows, MIT, Linux, Unix and OS X use MIT, CableLabs implementation for cable TV
 - User login, file access, printing, etc.

Basic Kerberos 5

- Authentication
 - Repeatedly authenticate a client to multiple servers
- Client *C* wants ticket for end server *S*
 - Tickets are encrypted - unreadable by *C*
- *C* first obtains long term (e.g., 1 day) ticket from a Kerberos Authentication Server *K*
 - Makes use of *C*'s long-term shared symmetric key
- *C* then obtains short term (e.g., 5 min.) ticket from a Ticket Granting Server *T*
 - Based on long term ticket from *K*
 - *C* sends this ticket to *S*

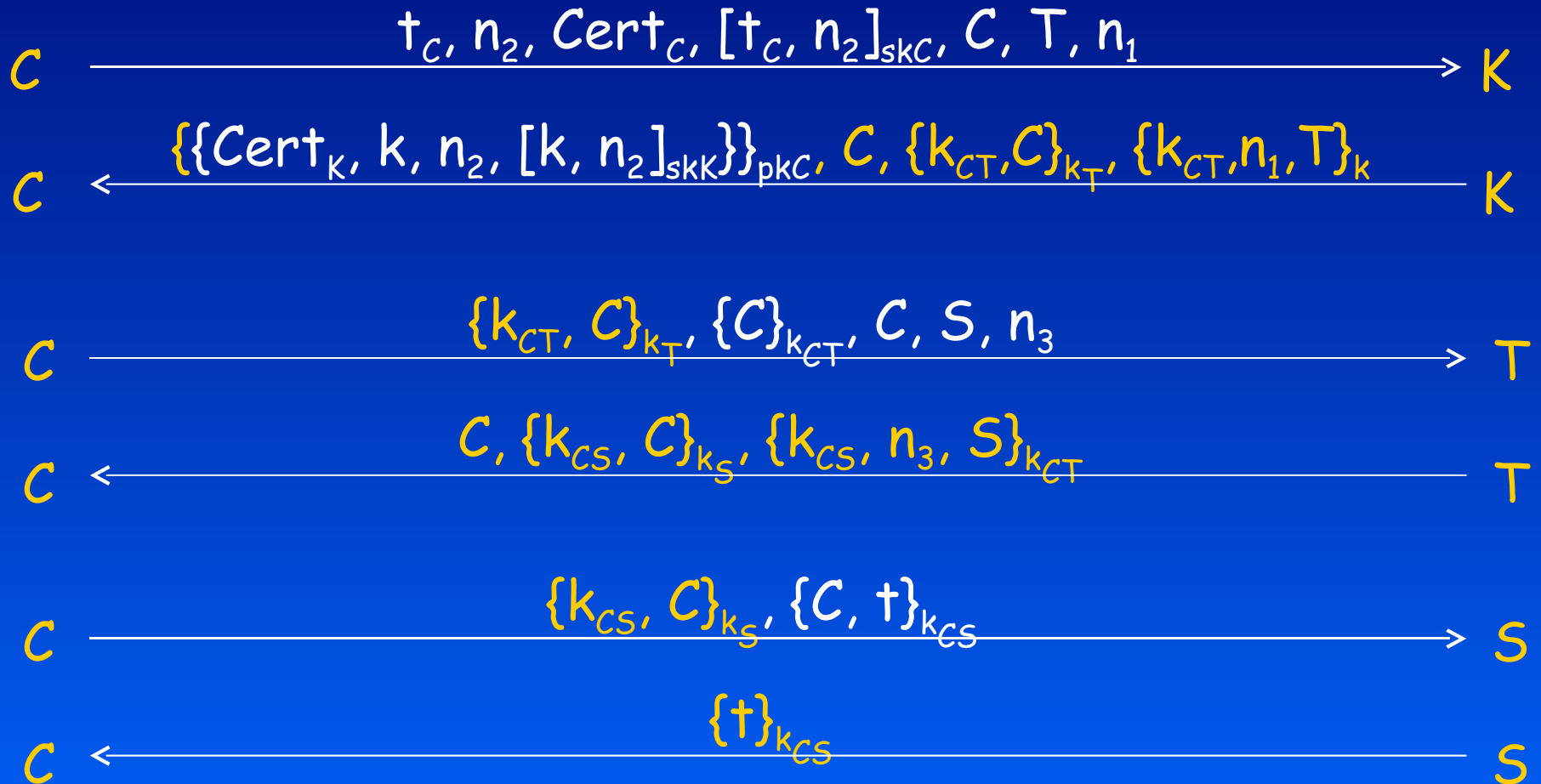
Public-Key Kerberos

- **Extend basic Kerberos 5 to use PKI**
 - Change first round to avoid long-term shared keys
 - Originally motivated by security
 - If Kerberos server is compromised, don't need to regenerate shared keys
 - Avoid use of password-derived keys
 - Current emphasis on administrative convenience
 - Avoid the need to register in advance of using Kerberized services
- This extension is called PKINIT
 - Current version is PKINIT-28
 - We found attack in -25; -26 does not change the relevant design
 - Versions included in Windows and Linux (called Heimdal)
 - Implementation developed by CableLabs (for cable boxes)
 - Apparently not in MIT version

Two Modes

- In general, no key k_c shared between C and K
 - Credentials for C instead encrypted under a temporary key k
 - How to generate and deliver k ?
- Public-key encryption
 - k is generated by K
 - k encrypted under C 's public key and is signed by K
 - Attack is against this mode
- Diffie-Hellman
 - k is generated by DH using data from C and K
 - C and K each send signed data to contribute to DH key
 - Option for 'reuse' of the shared secret
 - CableLabs appears to be only implementation of this
 - Initial inspection did not turn up attacks against this mode

Public-Key Encryption Mode



The Attack

At time t_c , client C requests a ticket for ticket server T (using nonces n_1 and n_2):

$C \xrightarrow{t_c, n_2, \text{Cert}_C, [t_c, n_2]_{skC}, C, T, n_1} I$

The attacker I intercepts this, puts her name/signature in place of C 's:

$I \xrightarrow{t_c, n_2, \text{Cert}_I, [t_c, n_2]_{skI}, I, T, n_1} K$

Kerberos server K replies with credentials for I , including: fresh keys k and AK , a ticket-granting ticket X , and K 's signature over k, n_2 :

(Ignore most of enc-part) $I \xleftarrow{\{k, n_2, [k, n_2]_{skK}\}_{pkI}, I, X, \{AK, \dots\}_K} K$

I decrypts, re-encrypts with C 's public key, and replaces her name with C 's:

$C \xleftarrow{\{k, n_2, [k, n_2]_{skK}\}_{pkC}, C, X, \{AK, \dots\}_K} I$

- I knows fresh keys k and AK
- C receives K 's signature over k, n_2 and assumes k, AK , etc., were generated for C (not I)

- Principal P has secret key sk_P , public key pk_P
- $\{msg\}_{key}$ is encryption of msg with key
- $[msg]_{key}$ is signature over msg with key

Real-World Impact

- Our work cited in August 2005 Microsoft security bulletin

www.microsoft.com/technet/security/bulletin/MS05-042.msp

- Although other vulnerabilities viewed as more pressing for IT managers, this attack has real-world effects and highlights a design vulnerability
 - Remote code execution, privilege elevation seem to arise from coding errors, not design flaws
 - No known exploit using our attack

Interactions with IETF

- Close collaboration with IETF Kerberos WG
 - Discussed possible fixes we were considering
 - Attack announced on WG list in July 2005
 - We verified a fix the WG suggested
 - This was incorporated into PKINIT-27
 - Presented this work at IETF-63
 - Discussed possible fixes and our analysis of these
 - Useful discussions with WG participants on other areas for work
 - Participating in WG meetings in Sept. and Nov. 2005
- Impact of formal methods in IETF security area
 - At security-area level, they want to see more interaction with formal methods



Software Quality and Infrastructure Protection for Diffuse Computing

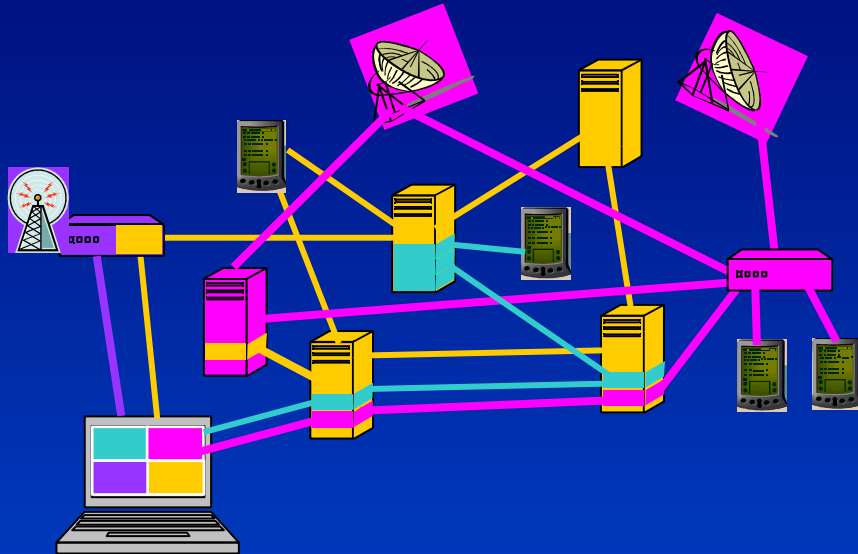
U Penn, Stanford, Cornell, Yale

URI, May 2001

Email: scedrov@math.upenn.edu

WWW: <http://www.cis.upenn.edu/spyce>

Nov. 10, 2005



Scientific Accomplishments

- Interdomain routing
 - Path vector protocols [Penn-Yale-Intel]
 - Local conditions for stable routes [Yale]
- Analysis of cryptographic protocols
 - Formal methods for cryptography [Penn-Stanford]
 - Kerberos 5 analysis [Penn-NRL]
- Logic for reasoning about policies [Cornell]
- SPAM reduction algorithms [Microsoft-Stanford]
- Privacy in databases [SRI-Microsoft]
- Anonymity and information hiding [Cornell-NRL]
- Content transcoding for heterogeneous clients [Penn]
- Flexible Lightweight Active Measuring Environment [Penn]

Educational Accomplishments

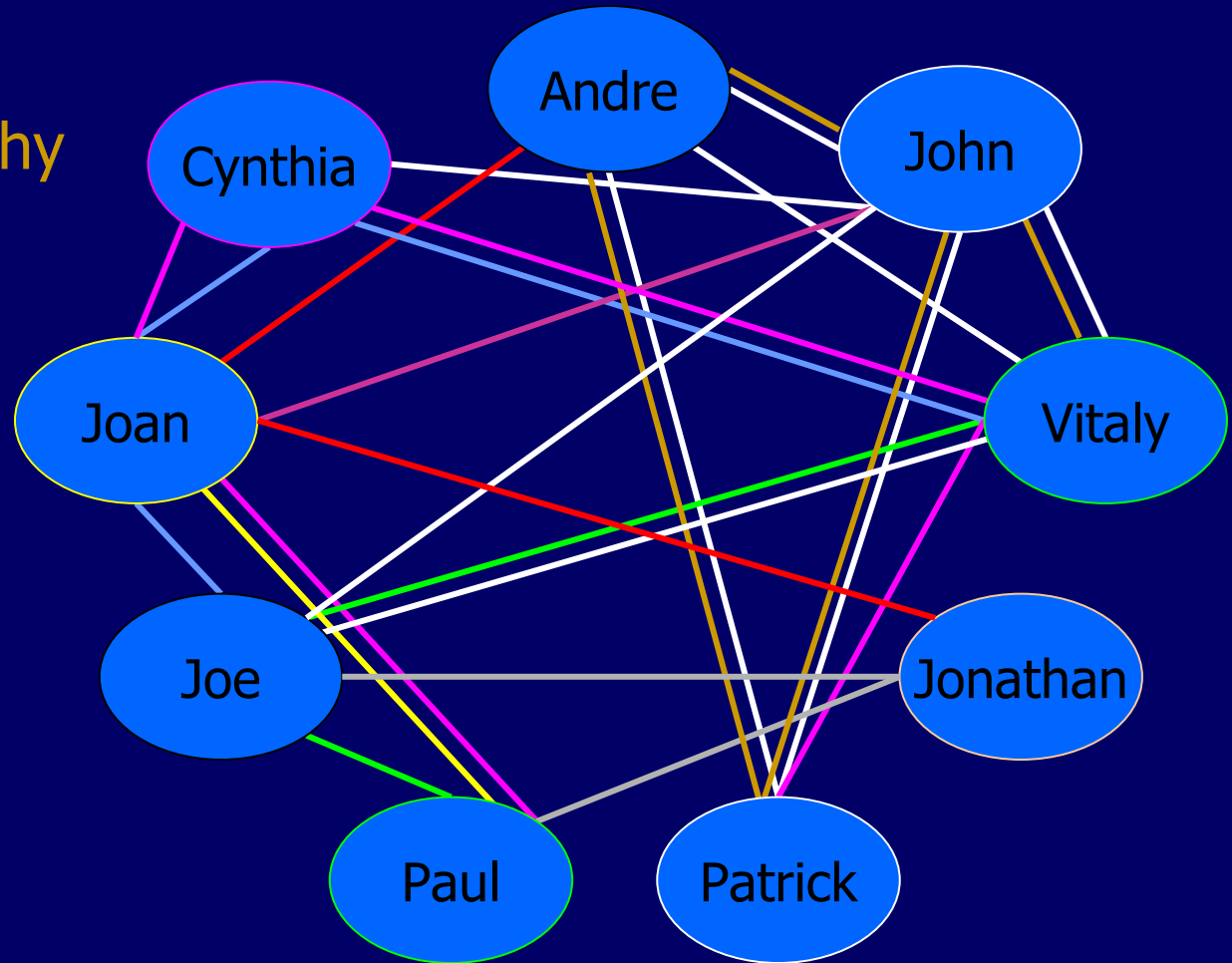
- Enhanced the ability to educate and train students in science and engineering and perform CIP/SW relevant research
 - 14 refereed journal publications
 - 65 refereed conference proceedings
 - 5 prototypes
 - 14 PhD students graduated, 22 PhD students supported
 - Members of NAS Computer Science and Telecommunications Board, Defense Science Board Task Force on Science and Technology, ACM Fellows, AAAI Fellows, ...

Project Contact Information

- PI: Prof. Andre Scedrov
 - co-PIs: Prof. Joan Feigenbaum,
Prof. Joseph Halpern,
Dr. Patrick Lincoln, Prof. John Mitchell
- Prof. Andre Scedrov
 - Department of Mathematics
 - University of Pennsylvania
 - 209 South 33rd Street
 - Philadelphia, PA, 19104-6395

Spyce Interaction Graph

- Protocol Analysis
- Formal Methods
for Cryptography
- Anonymity
- Privacy
- Algorithmic
Mech Design
- Authorization
- Decision Theory
- Networking
- Digital Rights



Recent SPYCE Dissertations

● Stanford

Ajith Ramanathan, Anupam Datta, Vanessa Teague

● Penn

Kostas Anagnostakis, Gergei Bana
MA Thesis: Jennifer Strong

● Yale

Vijay Ramachandran, Jian Zhang

● Cornell

Riccardo Pucella, Vicky Weissman

Today

- Impossibility result in cryptography

- Anupam Datta, Stanford Stanford - Penn

- Policy languages and reasoning about policies

- Vicky Weissman, Cornell Cornell - Stanford

- Networking

- Vijay Ramachandran, Yale Yale - Penn