IEEE
International Conference
on
PKI and Its Applications
(PKIA-2017)
November 14-15, 2017

Hotel Chancery Pavilion, Bangalore

# Digital Token Based Remote Administration

Presenter:
Anoop Kumar Pandey
C-DAC Bangalore

# Agenda

- Introduction
- Motivation
- Our Approach
- Security
- Simulation
- References

# Introduction

**Definition**

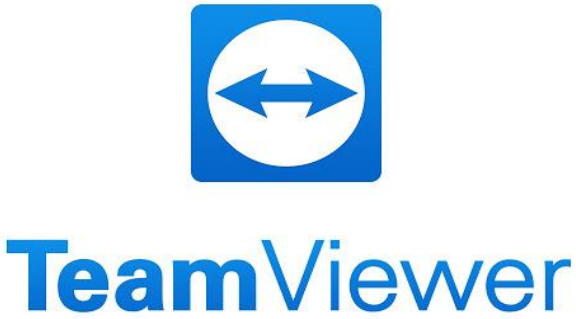
A method that allows remote access of a computer system pretty much similar to physical access.

**Methods/Forms**

- Commandline (SSH)
- Remote Desktop (RDP)
- Network File Browsing (FTP, NFS)
- Screen Capture

# Introduction (Contd.)

## GUI Tools



## Command line Tools

- Telnet, SSH
- Serial

# Introduction (Contd.)

## Web Based Tools


# Introduction (Contd.)

**Why??**

- Cost Benefit
  - 24*7 business but less employee
  - Onsite shortage of personnel
  - Lack of skilled personnel
- Productivity, Ease of Work, Efficiency
  - Work from Home

Security and Management Overheads??

# Problem with Existing Solutions

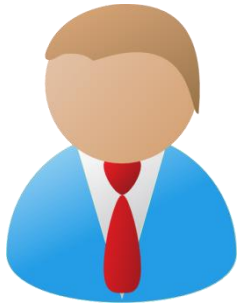
- Manual Supervision
- Privileges

# Proposed Solution

- A Digital Token
  - Cryptographically created
  - Holds validity period
  - Holds privilege
  - Issued to specific entity
- **Issue, Use, Keep Using, Purge/Expire**

# Issuance

Server (S)



Remote Administrator (R)

I = {PubKey(R), StartTime, EndTime, Priv}

ServerSign = Sign (I, PvtKey(S))

DigTok = {I, ServerSign}

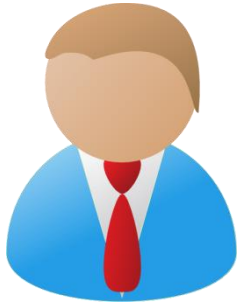
SDigTok = Encrypt(DigTok, PubKey(R))

**SDigTok** →

DigTok = Decrypt(SDigTok, PvtKey(R))

# Usage

Server (S)



Remote Administrator (R)

RSign = Sign(DigTok, PvtKey(R)

Rsign, DigTok

ServerSignVerify = Verify(ServerSign, PubKey(S), I)

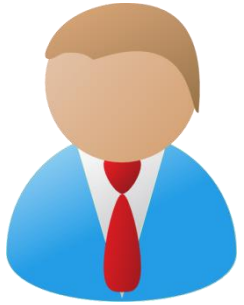
RSignVerify = Verify(RSign, PubKey(R), DigTok)

TimeCheck = Validate Time Period

If (RSignVerify & ServerSignVerify & TimeCheck)

# Impersonation

Server (S)



Remote Administrator (R)

ASign, DigTok

Imposter/Adversary (A)

ServerSignVerify = Verify(ServerSign, PubKey(S), I)

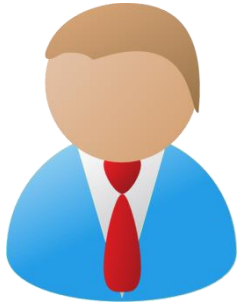
RSignVerify = Verify(ASign, PubKey(R), DigTok) where PubKey(R) is included in I

RSignVerify == TRUE/FALSE??

ASign = Sign(DigTok, PvtKey(A))

# Replay Attack

Server (S)



Remote Administrator (R)

I = {PubKey(R), StartTime, EndTime, Priv}

Replay by R!!
Who Cares??
How Long??

Adversary (A)

# Simulation

- Resoure: Pi Camera (Raspberry Pi 3 Board with attached Pi Camera )
- Method: Web Based
- Technology: RSA keygen and python scripts
- Results:

| Operations | Durations |
|---|---|
| Generating Key Pair (Client Side) | 4.9s |
| Generating Digital Signature on Data | 0.9s |
| Encryption of Data | 0.36s/1.1KB |
| Decryption of Cipher text | 0.104s |
| Verification of Data | 0.32s |

# References


[1] Command Line Interface, http://docs.oracle.com/cd/E19150-01/820-1855-13/cli_com.html#0_67209

[2] TeamViewer, https://www.teamviewer.com

[3] GoToMyPC, https://get.gotomypc.com/

[4] Remote Desktop Protocol, https://en.wikipedia.org/wiki/Remote_Desktop_Protocol

[5] Bhatt, Rupal, and D. B. Choksi. "A Comparative Evaluation of Remote Administration Tools." International Journal of Advanced Research in Computer Science 4.4 (2013).

[6] AnyDesk, http://anydesk.com/

[7] Rivest, Ronald L., Adi Shamir, and Leonard Adleman. "A method for obtaining digital signatures and public-key cryptosystems." Communications of the ACM 21.2 (1978): 120-126.

[8] Public Key Infrastructure, https://en.wikipedia.org/wiki/Public_key_infrastructure

[9] Chokhani, S., Ford, W., Sabett, R., Merrill, C., & Wu, Internet X. 509 public key infrastructure certificate policy and certification practices framework. No. RFC 3647. 2003.

[10] CERT, Configure computers for secure remote administration, 2000, URL: http://www.cert.org/ securityimprovement/practices/p073.html

CCA

IEEE
PKIA-2017

# Thank You

CDAC