Private and Secure Communication with an Adversarial Insider

Yvo Desmedt

Univ. of Texas at Dallas
USA

University College London
UK

June 18, 2013

Yvo Desmedt was partially supported by DARPA F30602-97-1-0205, NSF CCR-0209092, EPSRC EP/C538285/1 and BT as BT Chair of Information Security.

1. The enemy is inside

Since 1946 the British knew about the “atomic spies” at Los Alamos (see e.g., the arrest of Allan Nunn May). Many more got arrested later.

It seems the West has still not understood that:

The enemy is inside

Indeed, we now have many examples, such as Kim Philby (defected to the Soviets in 1963), . . .

Harsh pre-trial punishments, as solitaire confinement (Bradley Manning) has not helped (see Edward Snowden).

Since 1987, my main line of research has been on finding techniques to secure IT systems in which we assume that the enemy is inside. So, I helped, for example, to develop:

- Threshold cryptography, in which one cannot trust all devices that will be used for decryption or for signatures, either because:
  - their keys may have been compromised, or
  - the manufacturer may have become an adversary, or
  - the machine has been hacked.

In this lecture, we will survey some of the research done to design communication systems in which:

- the manufacturer may have become an adversary,
- the equipment has been hacked.

The design allows for the possibility not to know in advance who the adversary will be, a concept borrowed from the reliability community (see further for details).

2. Why is this important in the communication context?

We give just two examples:

1. DigiNotar
2. BT's use of of Huawei equipment

DigiNotar dies from certificate hack caper - Computerworld – Konqueror

File Edit View Go Bookmarks Tools Settings Window Help

Home Page Reload Stop Cut Copy Paste Print

DigiNotar dies from certificate hack caper

. . .

By Gregg Keizer
September 21, 2011 04:09 PM ET
2 Comments

Share Like 1

Computerworld - The Dutch company that was hacked earlier this summer by certificate thieves has gone bust and shut down, its U.S.-based owner said Tuesday.

. . .

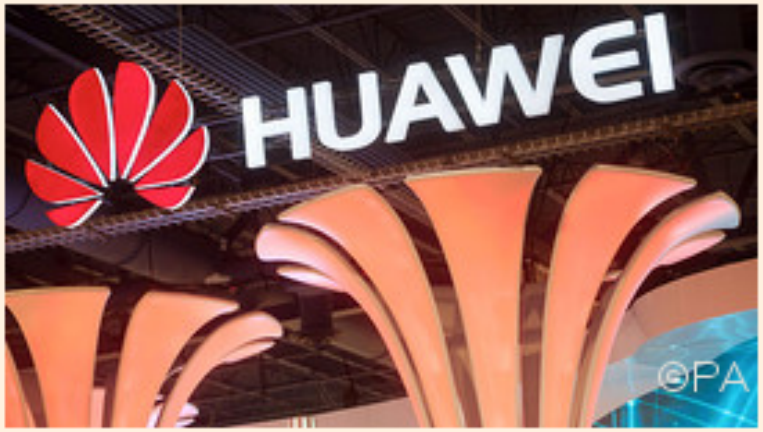
DigiNotar confirmed that it had first discovered the intrusion on July 19, but had not disclosed the breach to browser makers, the Dutch government -- which used DigiNotar certificates to validate the identities of many of its websites -- or other customers until more than a month later.

An investigation sponsored by the Dutch government revealed that the hacker or hackers first compromised DigiNotar's servers in mid-June and made off with more than 500 certificates.

Last updated: June 6, 2013 8:04 pm

UK security committee 'shocked' over Huawei contract with BT

By James Blitz and Daniel Thomas



A parliamentary committee has attacked the British government's failure to investigate the use of equipment from China's Huawei in the UK national telecommunications network, saying security issues "risked being overlooked".

ybel
edded in
s
ity under
utiny
ber warfare
PIC
ises lack of
Huawei
casts
ofit growth
affirms
Huawei
view
cott urged
ICS &
from
the timing
Hester in
exit
ils plans to

However, the committee, which comprises leading politicians and civil servants, said there would always be risks involved in any telecoms system sourced from abroad – and the UK authorities were not doing enough to manage that risk.

The committee said its investigation revealed "a disconnect between the UK's inward investment policy and its national security policy."

In particular, it said a centre set up by the government to monitor the physical equipment and software used by Huawei, "is highly unlikely to provide, or to be seen to provide, the required levels of security assurance".

3. Denial of service during communication: the issues

There are several issues, depending on:

The type of network. We distinguish:

Point-to-point networks

(Partial) broadcast

The type of adversary. We have:

Passive adversary has control to a subset of nodes and/or links. The adversary has access to all information received by these nodes (and all secrets of these nodes).

Active adversary. The nodes over which the adversary has control can behave in a Byzantine way. This means they can decide, not

to forward information, modify, not follow the protocol, follow the protocol, etc.

Destroyed nodes, (fail-and-stop) i.e. just stops communicating.

Jamming adversary in the case of (partial) broadcast, a third party can prevent communication between two parties.

The nodes controlled by the adversary. These can be specified by

a threshold. A t-bounded adversary can control up to t nodes.

an adversary structure. Let V be the nodes in the network. An adversary structure $\mathcal{A}_V$ over V is a subset of the power set 2^V such that if $B \in \mathcal{A}_V$ then subsets of B are also in $\mathcal{A}_V$.

The level of security. We distinguish between:

Perfect (see further).

δ**-reliability,** i.e. with probability at least $1 - \delta$, B terminates with the same message as A sent.

ε**-privacy.** Unconditional security (See literature: Franklin-Wright.) Edge: considered private communication.

The perfect case corresponds to $\delta = 0$ and $\varepsilon = 0$.

The security of sender/receiver We distinguish between the case the sender and/or receiver:

- can use trusted equipment
- can not use trusted equipment

Decisional versus search. We distinguish between:

Decisional questions: given a network, does it allow the desired security against a type of adversary? So, issues are:

- necessary and sufficient conditions
- if possible, what protocol do the participants run
- an algorithm for deciding, or
- proving the problem is hard (e.g. **NP**-hard).

Computational questions , in particular:

Construct a network for the desired security against a type of adversary with parameters, e.g. number of nodes is given. Issues:

Bounds: Necessary conditions

Constructions: Sufficient conditions

Update a network. Start from existing network (satisfying a security property). How to update it (with minimum "cost") so it satisfies a (new) security property?

4. Complexity of the problem: illustration

What about the following solution:

Send a message using standard techniques (TCP), when not receiving an acknowledgment, then the adversary must have control over the communication path. Use a different path then.

This technique does not work

(except when using end-to-end authentication, which is non-trivial without the use of a PKI, which is itself a "directed graph" (of which computer signs someone's else public key)).

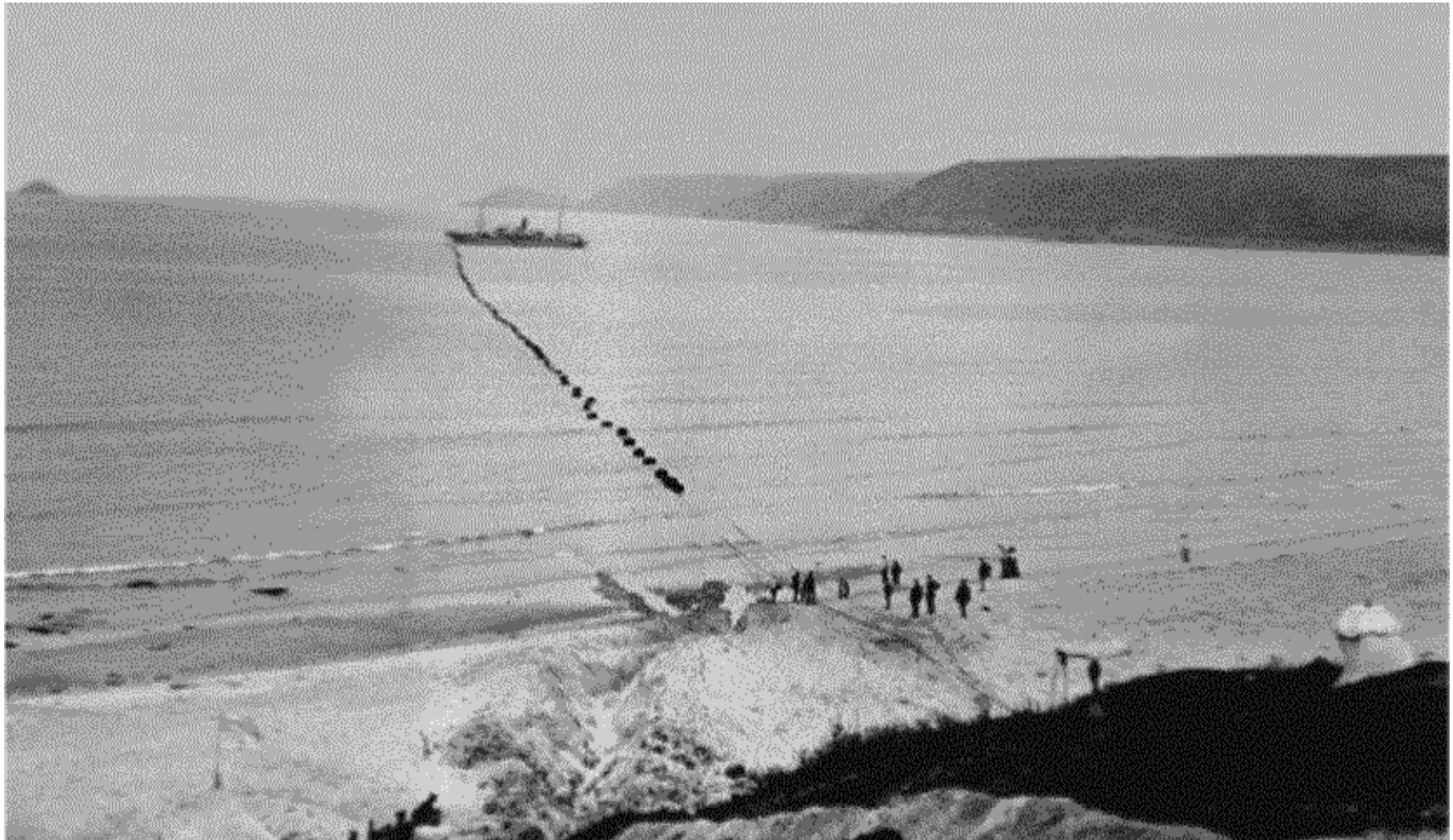
Indeed, the adversary will just send a fraudulent ACK to the sender.

The solutions borrow from the reliability community. As an example:

When you fly an airbus, 3 computers compute fuel consumption, route, etc. all the time!

5. Classical results

This goes back to World War I, after the cable ship Telconia lifted from the bed of the North Sea the German overseas telegraph cables:



If an adversary can destroy t nodes, then $t+1$ vertex disjoint paths are needed and sufficient to communicate from sender (node A) to receiver (node B). If any two non-destroyed nodes want to communicate, it is necessary and sufficient that the directed graph must be strongly $t+1$ connected.

Illustration: node disjoint paths: a closed station

If the adversary can be Byzantine, then one needs $2t + 1$ vertex disjoint paths, respectively $2t + 1$ connectivity.

Dolev-Dwork-Waarts-Yung (1993) added privacy. They required perfect reliability, and perfect privacy.

6. POINT-TO-POINT NETWORKS

- Sender/receiver equipment is trusted:
  - Point-to-point: threshold adversary:

    Dolev-Dwork-Waarts-Yung (1993) considered:

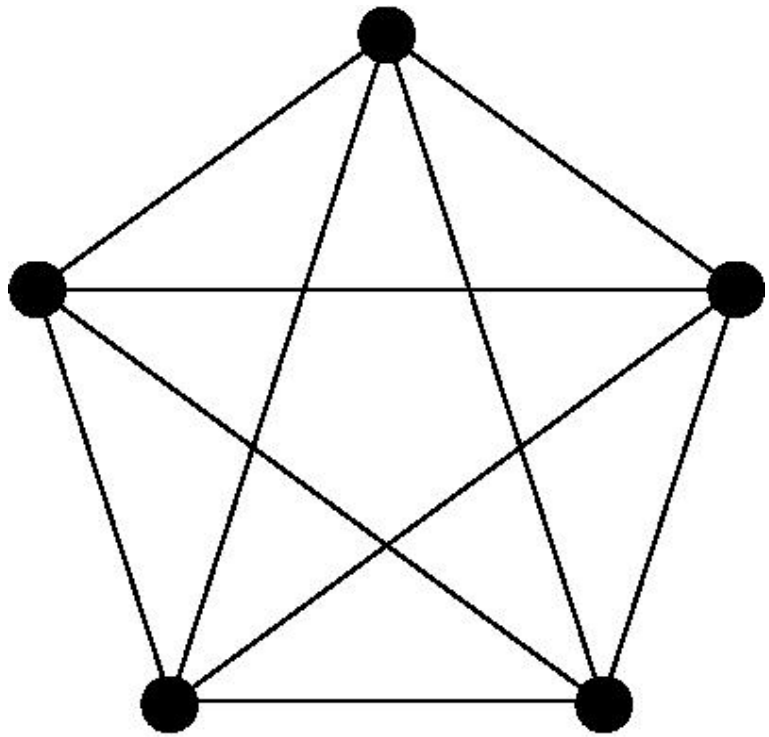
    all communication links (edges in the graph) are:

    one-way without feedback. It is necessary and sufficient to have $3t + 1$ vertex disjoint directed paths from A to B (for any two nodes: the graph must be $3t + 1$ connected).

    Definition 1. A graph is (vertex) 1-connected if there is a path from every vertex to every vertex. When $k > 1$, a graph is k-connected if after the removal of any single vertex (and its adjacent edges) remains $(k - 1)$-connected.

Theorem 1. *A graph is k-connected if and only if between any two vertices A and B there are k vertex disjoint paths.*

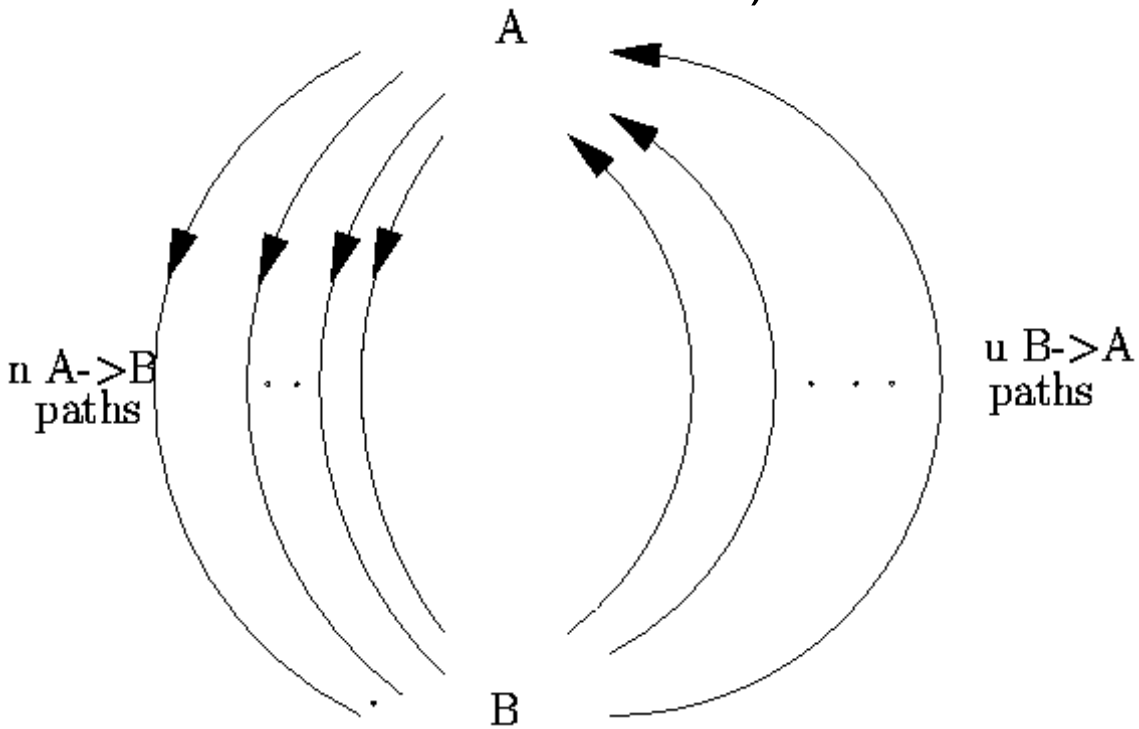
Example:



two-way. $2t + 1$ vertex disjoint paths are necessary and sufficient.

Their algorithm was inefficient. It took until 2008 until it was made practical (Kurosawa-Suzuki).

Desmedt and Wang (2002) observed this above are not the most general cases, since there could be feedback channels. They focused primarily on the case the feedback channels are vertex disjoint from the forward channels. (Several follow papers improved on some of these results.)



– Point-to-point: general adversary What is a general adversary structure?

Given a set P (e.g., of nodes and links), one specifies what subsets might behave maliciously. So, as stated earlier:

The design allows for the possibility not to know in advance who the adversary will be.

This prevents preparing everything for a full blown war with the Soviets, and then being attacked by Al Qaeda on September 11, 2001.

Example set $P = \{1, 2, 3\}$ and $\mathcal{A}_P = \{\{1\}, \{2, 3\}, \{2\}, \{3\}, \emptyset\}$.

Maximal adversary set: $\mathcal{A}_P^* = \{\{1\}, \{2, 3\}\}$.

Applied to communication:

Let A and B be the sender and receiver. Let

$Z_1, Z_2, Z_3 \in \Lambda_{V \setminus \{A,B\}}$.

A necessary and sufficient condition for A and B to privately communicate in the presence of a Byzantine adversary, in the case all communication links (edges in the graph) are:

two-way that removing any nodes specified by any $Z_1 \cup Z_2$ (see above) A, B remain connected (Kumar-Goundan-Srinathan-Rangan, 2002).

one-way without feedback, that removing any nodes specified by any $Z_1 \cup Z_2 \cup Z_3$ is that A, B remain connected (Desmedt-Wang-Burmester, 2005).

Necessary and sufficient conditions for privacy-only and perfect reliability-only were given in Desmedt-Wang-Burmester, 2005. (See also Yang-Desmedt, for efficiency improvements.)

- Sender/receiver equipment is untrusted: (e.g., when the country is technological challenged, or has outsourced all its production of electronics).

  Two cases were studied:

  – Non-interactive $\mathrm{mod}10$ with a human receiver

  – Two-phase $\mathrm{mod}10$ with a human receiver

  Moreover, a method to add $\mathrm{mod}10$ in a human friendly way was proposed and human experiments confirmed its ease.

  For details: Erotokritou-Desmedt 2012.

7. PARTIAL BROADCAST

- The general case

  Franklin-Yung (1995,2004) replaced the point-to-point network by a partial broadcast. They use a directed hypergraph. A directed hypergraph $H = (V, E)$ consists of set of vertices V, however a directed hyperedge $e \in E$ has the form (v, V'), where $v \in V$ and $V' \subset V$. When the node v uses this directed hyperedge all nodes in V' receive the same information (others learn nothing about that information).

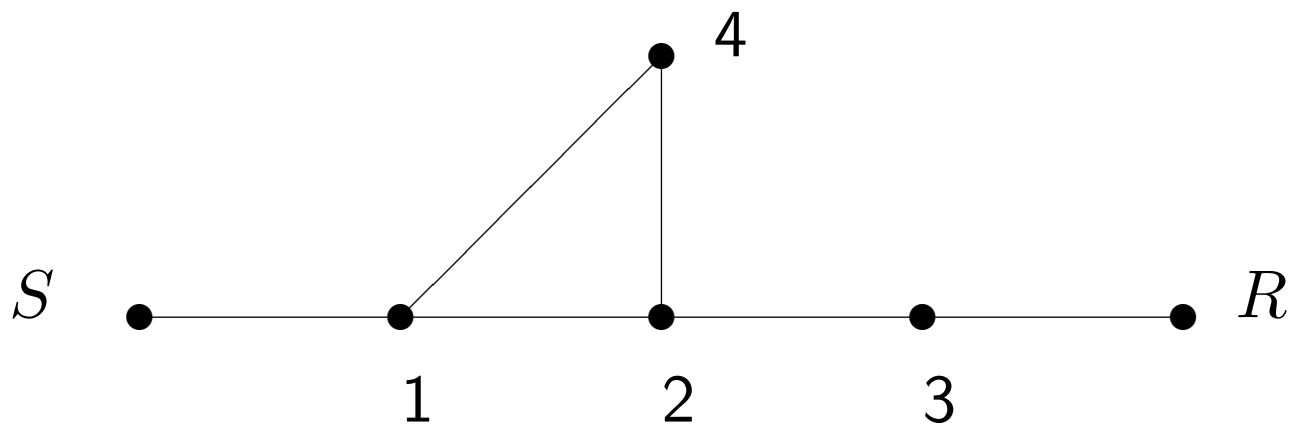
  For the threshold case, Franklin-Yung gave necessary and sufficient conditions for privacy-only.

- Partial broadcast: the multicast case

  Franklin-Yung also introduced special cases, one of these is called a neighbor network, which can be represented by an ordinary graph. Ethernets are a special case of these.

  In this graph if a vertex broadcast a message, all its neighbors will receive identically the same information.

  Example:



  If node 2 sends u, 1, 3, and 4 receive the same u. Using Franklin-Yung 1995 terminology, $(2, \{1, 3, 4\})$ is a directed hyperedge in which 2 is broadcasting.

Necessary and sufficient conditions for privacy and reliability were an open problem since 1995 and were finally solved in 2011 (Yang-Desmedt).

8. Potential applications

We give two examples:

- PKI:

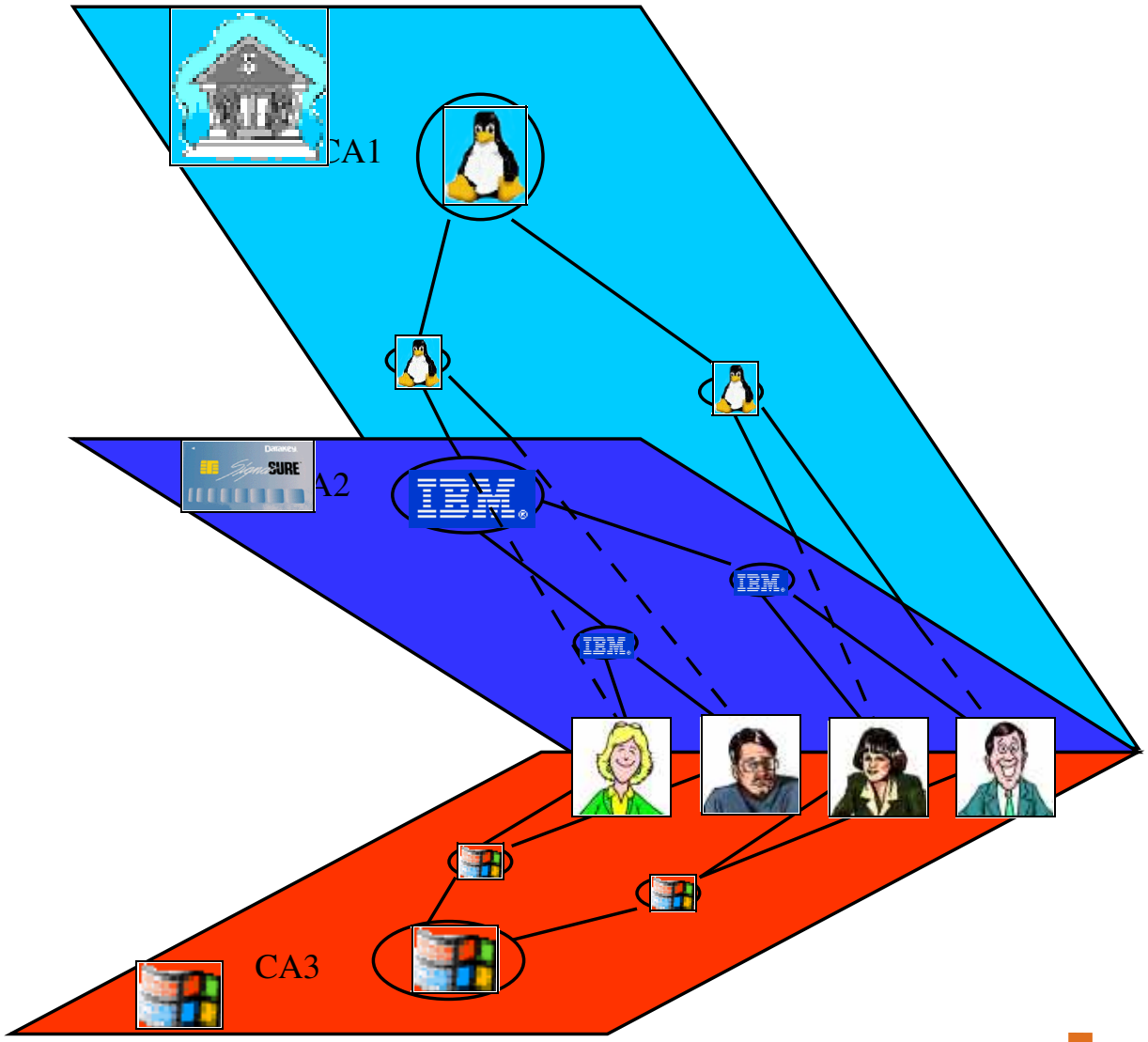
  PKI is the foundation of electronic commerce. It is supposed to guarantee the correctness of the public keys used in secure modern communication.

  In 1996 Burmester-Desmedt-Kabatianskii and independently in 1997 Reiter-Stubblebine pointed out that in the currently deployed PKI every node is a single point of failure (from a security viewpoint). An alternative, also hierarchical in nature, as the current PKI was proposed by Burmester-Desmedt in a paper with title

  Is hierarchical public-key certification the next target for hackers?

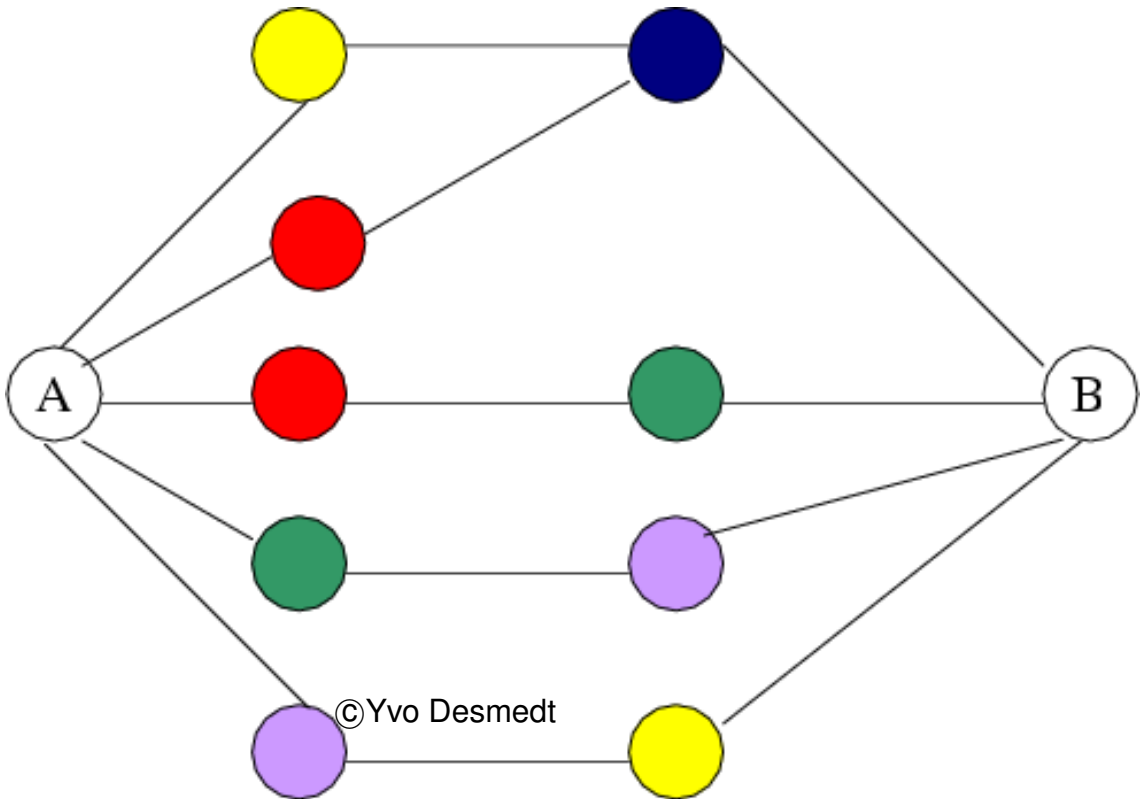
  in 2004 using “colors” to model CA platforms that could be hacked.

Each node's (CA's) platform is indicated by coloring the node. We proposed in particular:



- Building point-to-point networks with untrusted equipment
  - Node level:

    As earlier, we color the nodes dependent who built a particular router (or other node equipment). We introduced what we called a k-color adversary structure. However, we realized that we cannot require to build networks in a similar way as we proposed for PKI. So, Desmedt-Wang-Burmester (2005) considered networks as:



* Positive result: whether we can achieve privacy and/or reliability, fits within the results on general adversary structures.
* Negative result: Desmedt-Wang-Burmester (2006) showed that deciding whether a "colored" graph is k-color connected, is Co-NP-complete.

– Link level:

The issue that has been addressed (Wang-Desmedt 2011) is fail-and-stop in which $k+1$ different modem technology is being used and t of these might fail one day.

9. Implementations

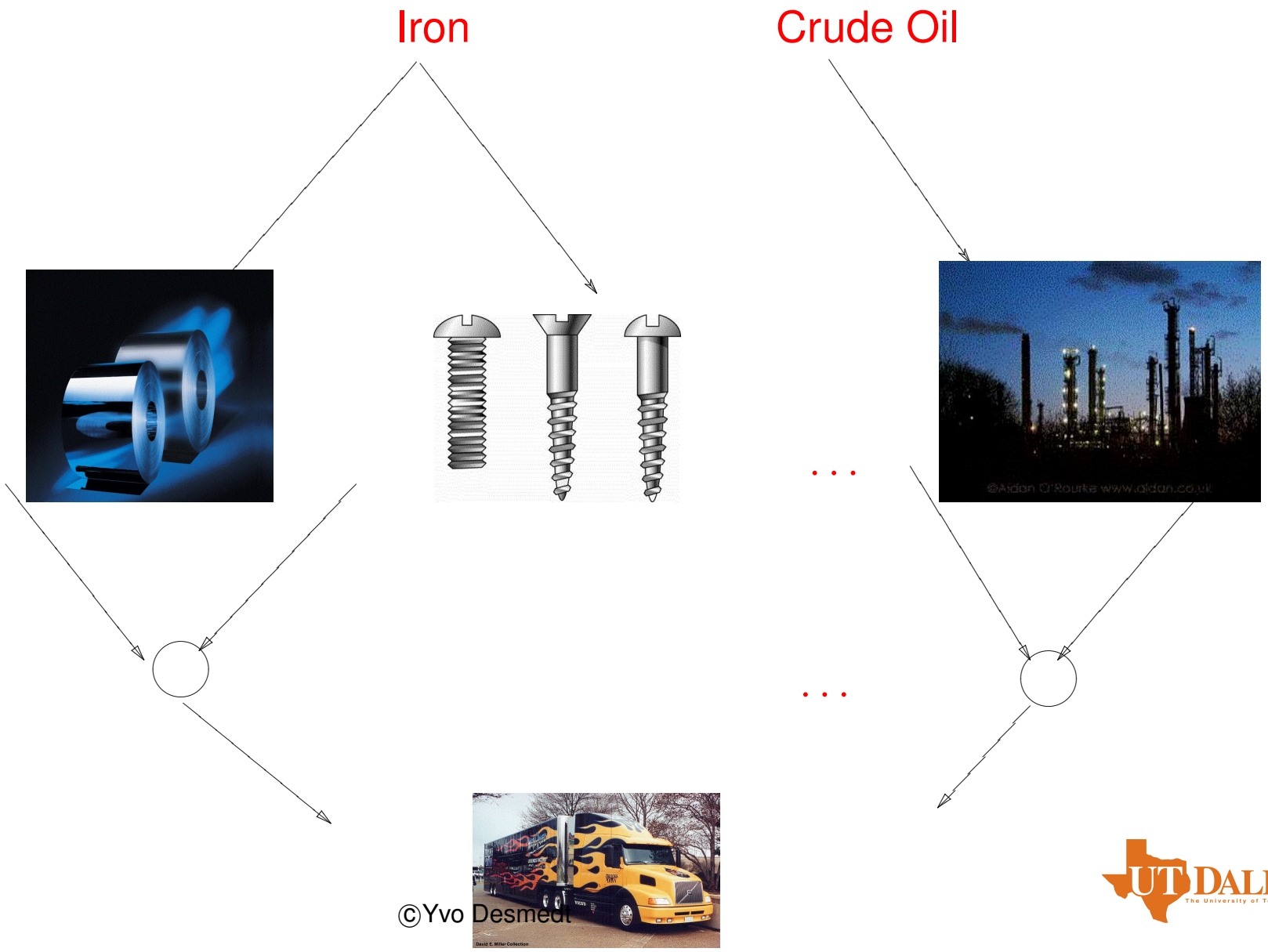
1. Erotokritou-Desmedt (unpublished) tried to implement the 1993 non-interactive solution of Dolev-Dwork-Waarts-Yung. The amazing problem we encountered is that:
   - the 1993 internet technology would had allowed a 1993 implementation,
   - the current internet technology no longer allows to implement this. Reasons:
     - to guarantee $3t + 1$ vertex disjoint paths, we must specify the path a data packet has to follow. Today any packet that uses the standard TCP/IP option to specify the path is dropped by modern routers!!

– companies want to keep the layout of the network private, which causes another difficulty!

2. Desmedt-Cheney (unpublished) designed and implemented a Thunderbird extension using mail servers, as gmail, hotmail, yahoo, etc. For example, gmail and hotmail are considered as intermediary nodes between the sender and receiver. So, we consider Google and Microsoft as potential adversaries, not working together.

10. Extensions

Example of an application:



11. Conclusions

Building inexpensive operating systems and outsourcing communication equipment comes at a price: one can no longer trust them!

However, for several decades solutions have been under research. Unfortunately, they come at a cost: such as the need for redundancy, and the need to reconsider the design of routers.

The cost of communication is getting low. Indeed, Google's Gigabit fiber is coming to Austin (now also AT&T). Sony is offering 2 Gigabit in the Tokyo area. So, (P)SMT, i.e., Perfectly Secure Message Transmission technology should be considered seriously. Moreover, it is easy today to have multiple providers (landline and mobile).

12. References

[1] M. Burmester and Y. G. Desmedt. Is hierarchical public-key certification the next target for hackers? *Communications of the ACM*, 47(8), pp. 68–74, August 2004.

[2] M. Burmester, Y. Desmedt, and G. Kabatianskii. Trust and security: A new look at the Byzantine generals problem. In R. N. Wright and P. G. Neumann, editors, *Network Threats, DIMACS, Series in Discrete Mathematics and Theoretical Computer Science, December 2–4, 1996, vol. 38*. AMS, 1998.

[3] Y. Desmedt. Unconditionally private and reliable communication in an untrusted network. In *IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security, Proceedings*, pp. 38–41, October 16–19, 2005. Awaji Island, Japan.

[4] Y. Desmedt and Y. Wang. Maximum flows and critical vertices in and/or graphs. In O. H. Ibarra and L. Zhang, editors, *Computing and Combinatorics, 8th Annual International Conference, COCOON 2002 (Lecture Notes in Computer Science 2387)*, pp. 238–248. Springer-Verlag, 2002. Singapore, August 15-17.

[5] Y. Desmedt and Y. Wang. Perfectly secure message transmission revisited. In L. Knudsen, editor, *Advances in Cryptology — Eurocrypt 2002, Proceedings*

(Lecture Notes in Computer Science 2332), pp. 502–517. Springer-Verlag, 2002. Amsterdam, The Netherlands, April 28–May 2.

[6] Y. Desmedt, Y. Wang, and M. Burmester. A complete characterization of tolerable adversary structures for secure point-to-point transmissions without feedback. In X. Deng and D. Du, editors, *Algorithms and Computation, 16th Annual International Conference, ISAAC 2005, (Lecture Notes in Computer Science 3827)*, pp. 277–287, 2005. December 19 - 21, 2005, Sanya, Hainan, China.

[7] Y. Desmedt, Y. Wang, R. Safavi-Naini, and H. Wang. Radio networks with reliable communication. In L. Wang, editor, *Computing and Combinatorics, 11th Annual International Conference, COCOON, Proceedings (Lecture Notes in Computer Science 3595)*, pp. 156–166, 2005. Kunming, Yunnan China, August 16-19, 2005.

[8] D. Dolev, C. Dwork, O. Waarts, and M. Yung. Perfectly secure message transmission. *Journal of the ACM*, 40(1), pp. 17–47, January 1993.

[9] S. Erotokritou and Y. Desmedt. Human perfectly secure message transmission protocols and their applications. In I. Visconti and R. De Prisco, editors, *SCN*,

volume 7485 of *Lecture Notes in Computer Science*, pp. 540–558. Springer, 2012.

[10] M. Franklin and M. Yung. Secure hypergraphs: Privacy from partial broadcast. *SIAM J. Discrete Math.*, 18(3), pp. 437–450, 2004.

[11] M. K. Franklin and M. Yung. Secure hypergraphs: Privacy from partial broadcast. In *Proceedings of the twenty seventh annual ACM Symp. Theory of Computing, STOC*, pp. 36–44, 1995.

[12] M. Kumar, P. Goundan, K. Srinathan, and C. Rangan. On perfectly secure communication over arbitrary networks. In *Proceedings of the Annual ACM Symposium on Principles of Distributed Computing (PODC)*, pp. 193–202, 2002.

[13] K. Kurosawa and K. Suzuki. Truly efficient 2-round perfectly secure message transmission scheme. *IEEE Transactions on Information Theory*, 55(11), pp. 5223–5232, 2009.

[14] M. K. Reiter and S. G. Stubblebine. Path independence for authentication in large scale systems. In *Proceedings of the 4th ACM Conference on Computer and Communications Security*, pp. 57–66, April 1997. Zurich.

[15] Y. Wang and Y. Desmedt. Perfectly secure message transmission revisited. *IEEE Transactions on Information Theory*, 54(6), pp. 2582–2595, 2008.

[16] Y. Wang and Y. Desmedt. Edge-colored graphs with applications to homogeneous faults. *Information Processing Letters*, 111(13), pp. 634–641, July 2011.