Nokia Telecom Council of Silicon Valley Global Innovation Challenge Demo Winner ! ! !

No - No - No - Nokia

- no cyber crime
- no fear
- no hassle

Whitenoise Laboratories Canada Inc.
André Brisson - Founder
July 2, 2014

Total Telco Security for

- Cloud
- Colossal Data - Secure data centers
- Analytics - Perfect identity and data provenance
- Secure enterprise and secure clients

NOKIA

No – No – No – Nokia: * no cyber crime * no fear * no hassle

One distributed Whitenoise OTP key eliminates all attacks and secures all data and networks

Problem

Cyber crime is the #1 national and personal security threat globally.

$445 billion cost to the global economy in 2013

Center for Strategic and International Studies

Solution

- One key creates an infinite number of one-time-pads
- One protocol (DIVA) eliminates all known cyber attacks
- One virtual framework (DDKI) is scalable, interoperable and works with any other security controls or frameworks.

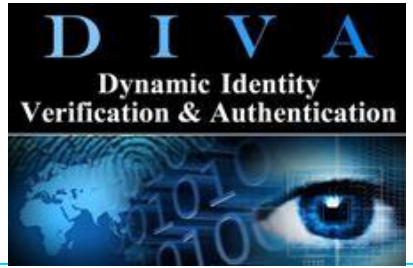
Benefits

User – no theft, no fear, no hassle

Operator - lower operating and infrastructure costs; new businesses and secure services with higher profit margins

Nokia – distinct, protectable competitive advantage

- virtually manufactured
- virtually provisioned



Current Status
- Commercial
- Entering large scale commercial

AT&T certified

Patented globally including Canada, US, EU, China, India. Brazil, Australia and Japan

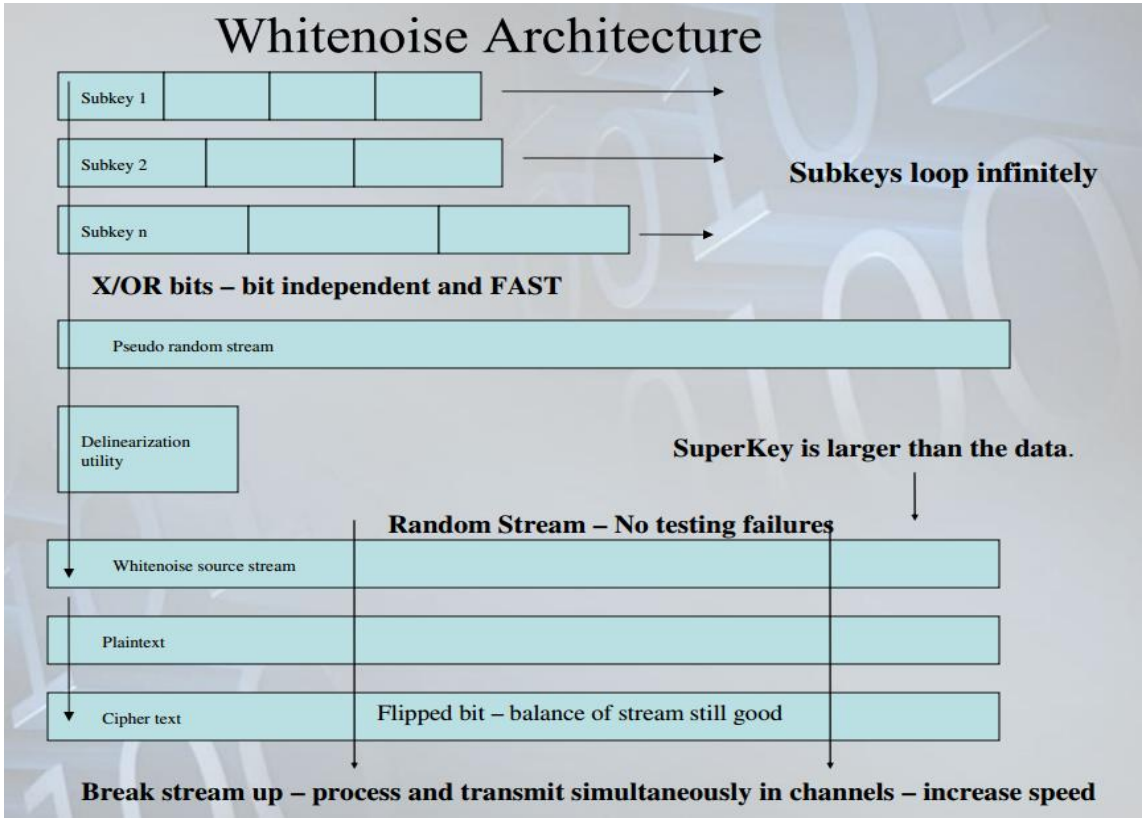
Vancouver, British Columbia

CIC Cambridge, Ma.

Incorporated 2008

NOKIA

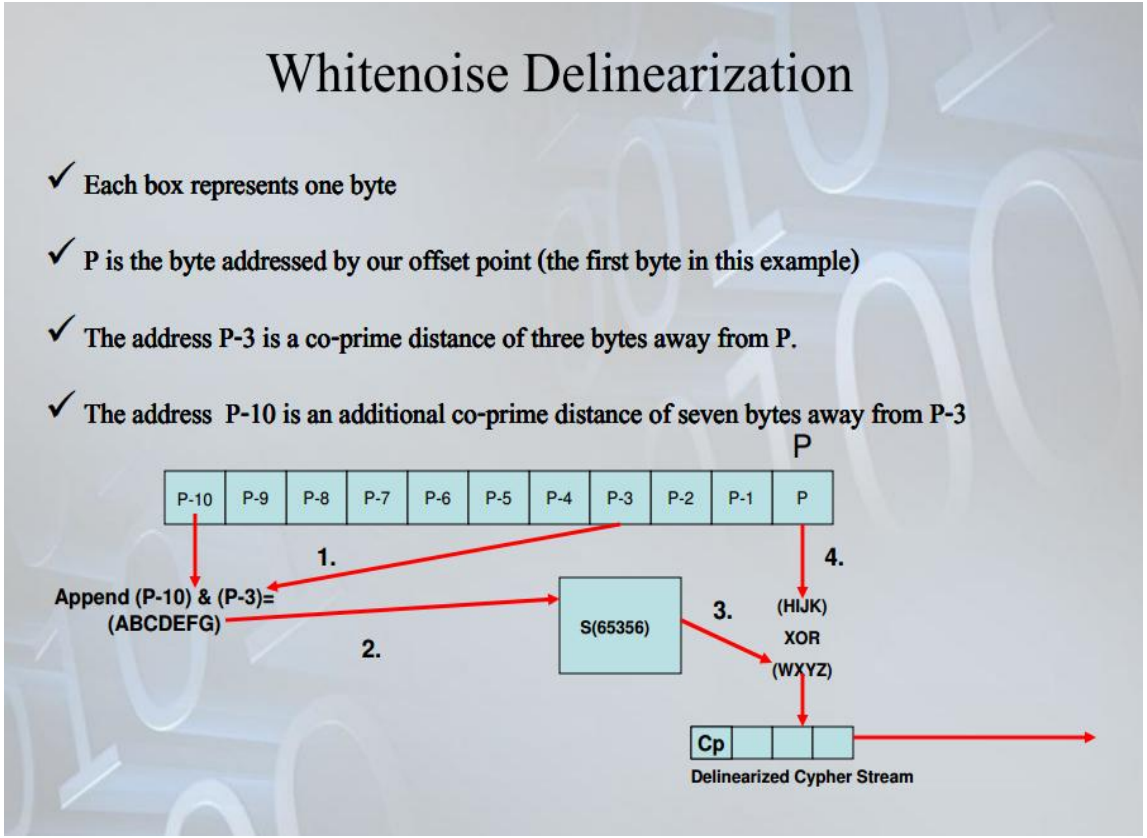
How is a Whitenoise key made?



- variable number of prime number length subkeys
- each bit is XOr'd with the corresponding bit of the next subkey
- it is run through an S-box to create a one-way function
- it becomes first byte of delinearized key stream

NOKIA

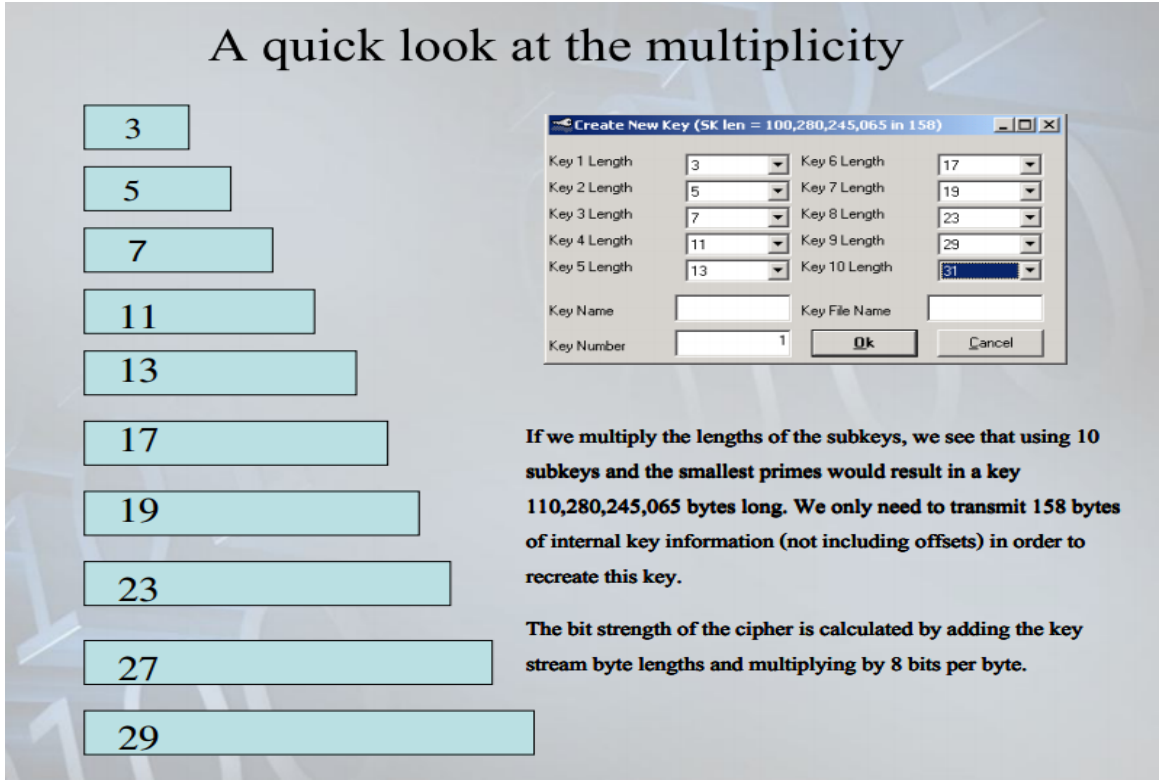
What are the Whitenoise one-way functions?



- two bytes are taken from the initial key stream, appended together and pushed through an S-Box
- only one byte emerges
- a hacker cannot go backwards and guess two bytes from one byte of information
- the hacker has no knowledge of the number of subkeys

NOKIA

How do I calculate the length and strength of a Whitenoise key?



- the length of a Whitenoise key is calculated by multiplying the length of the subkeys in bytes.

- the strength of a Whitenoise key is calculated by adding the lengths of the subkeys in bytes and multiplying by 8 bits per byte.

- we only have to store 158 bytes of information

NOKIA

How does Dynamic Identity Verification and Authentication protocol work?

Both server and endpoint have a copy of the account identity management key. The server sends a request to the endpoint for an identification token of a specific length, in this case twenty-five bytes. It is not sending across either an offset or a key with this request.

Last valid offset

Device state 1a

22 1F CB FE FA 17 F2 8E A5 F0 8A E1 55 D6 DD 36 13 73 E2 9A 65 2F F6 EA 71 FE F7 D7 B8 28 5D 26 8B 93 64 16 03

The key stream is a minimum of 10^{60} bytes in length. We are continuously and dynamically comparing tokens to insure the correct identity of the network user. A token is an unused segment of key stream of an arbitrary length. It is random and has the equivalency of being encrypted – it cannot be guessed or broken and it is only used once.

The endpoint replies by sending a 25-byte token beginning at its last valid offset.

Last valid offset plus token

Device state 1b

22 1F CB FE FA 17 F2 8E A5 F0 8A E1 55 D6 DD 36 13 73 E2 9A 65 2F F6 EA 71 FE F7 D7 B8 28 5D 26 8B 93 64 16 03

length = 25 bytes This is arbitrary and scalable depending on security requirements.

NOKIA

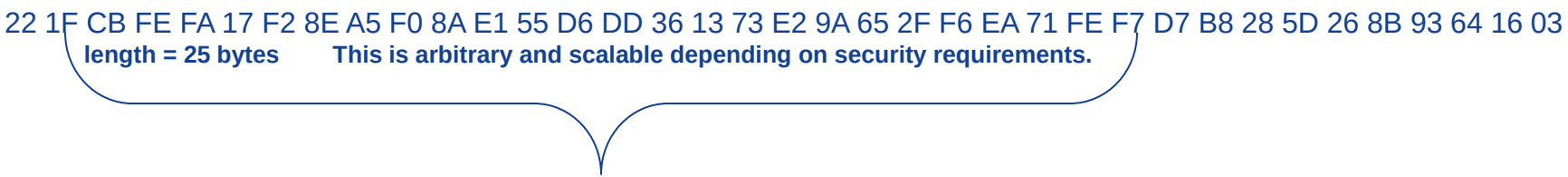
DIVA dynamic update of offset

Server authenticates user/device by comparing the received token bit-by-bit to the token generated at the server for this account/person/device. If they are identical then the

- **Server acknowledges by sending authorization**
- **Both server and endpoint update dynamic offset independently**

Last offset

New offset = last offset + token + 1

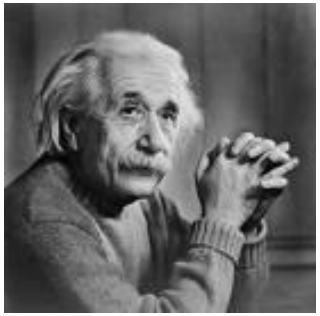


The system is synchronized for the next continuous authentication query.

The account is automatically locked if the comparison of tokens fails. This would happen if someone has copied a key and the offsets are not synchronous.

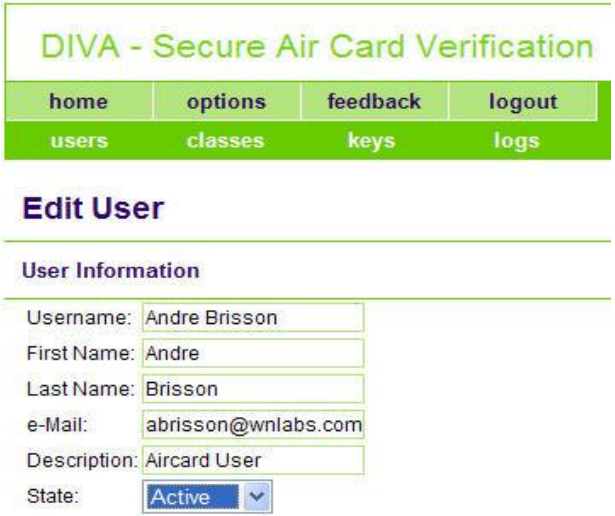
NOKIA

100 % accurate – only two DIVA outcomes



Someone tries to steal a key.

1. **The legitimate user logs back onto the network first.**

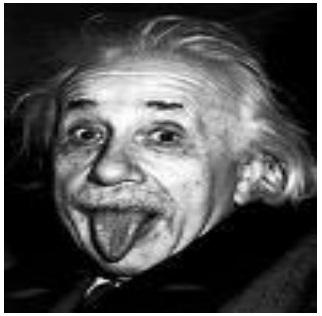


- **The legitimate key and server offset dynamically updates with this use independently.**
- **The pirated or spoofed key (if possible) is no longer synchronized with the server and the legitimate key.**
- **The pirate will be detected if he makes a login attempt.**
- **The pirate can't access network. Stolen copy is useless.**
- **No theft has occurred.**

This is the only outcome we have ever seen.

NOKIA

2. The pirate somehow steals a key and logs on first



Gotcha Hacker!

- The offset at the server and pirated key updates with this use.
- The legitimate key is no longer synchronized with the server.
- The next time the legitimate owner logs onto the secure network, the server recognizes that the offset is no longer synchronized because of the pirated key.
- The account is automatically locked.
- System Administrator and client know that their account has been accessed.
- The logs know the exact duration of the event and the exact transactions within that time beginning at the last time the server and client were synchronized and ending at the point in time when the account was locked.
- The pirate I P address is known for law enforcement use.

NOKIA

Two things you must remember about WN, DIVA and DDKI

It works seamlessly without direct integration with PKI and any other security frameworks or controls.

It is NOT only about encryption. That is a small part. Whitenoise technologies perform all network security controls with a single distributed key.

- perfect identity
- secure network access
- continuous dynamic authentication
- authorization
- signature
- non-repudiation
- inherent intrusion detection
- automatic revocation
- and yes, encryption

NOKIA

DDKI a virtual framework

Dynamic Distributed Key Infrastructures are secure, tiered, hierarchical virtual frameworks of devices and components deploying DIVA.

They are easily scalable and interoperable and have solved the traditional problems that have stopped large scale distributed networks of key storage and distribution. There is a one to one relationship between the keys at a server and endpoint. There is easy key storage and transfer because of multiplicity.

It is ideal for most things including Managed Mobile Networks and services and Scalable Adaptive Secure Networks.

NOKIA

DIVA prevents all known cyber attack classes

Man-in-the-Middle attacks are prevented because there is no key exchange.

Side Channel attacks are prevented because all operations are order 1 after key load and because there is no access to the key.

Mathematical and factoring attacks are prevented because keys are created mechanically as opposed to mathematically.

Botnet attacks are prevented by configuration with server so the botnet never has access to all the key material to authenticate data being sent OUT of a network or computer.

Quantum computing attacks are prevented because every variable is variable and that along with brute force attacks are prevented because the keys can’t be factored.

Denial of service attacks, I believe, can be prevented by exploiting unbreakable identity and secure network access so that hackers could never get on a network.

NOKIA

Proof of value: No - No - No Nokia

no latency; no added overhead; no accelerators; no maintenance; no training; no errors; no breaches; no complaints

Target customers: Telcos, utilities and critical infrastructure, transportation, all media, B2B, M2M, Internet of Things

Software/firmware Implementation cost is negligible. Add WN-DIVA algorithm to anything.

Client/endpoint – 20k storage; connectivity; write back. DB tracks key and current dynamic offset. Key firmware added electronically like Windows updates or to chipsets

Server – performs key distribution (1 time), enrollment, $ collection, authentication & activation. It performs security comparisons (inherently). A database tracks account, unique key structure, perfect IdM, secure network access, dynamic continuous authentication, authorization, signature, non-repudiation, DRM, encryption for DRM and other contexts, inherent intrusion detection and automatic revocation without human intervention. Flags SA for incidents and forensics for logs.

Market Universe: There are 7 trillion smart devices and components. Potential licensing revenue at just .01 per annum is $70 billion/yr or 5X Nokia 2013 revenue of 12.7 billion Euros. Revenue is annuitized for the life of the device, account or service. As an example, DoCoMo makes 25% of their profits from self running authentication services.

What is Nokia's role: Nokia provides internet services, financial services, applications, games, music, media, and messaging. Nokia Solutions and Networks provide telecommunication network equipment and services. Nokia can help make Microsoft a "SECURE devices and services company". Nokia can rapidly secure the world's critical infrastructures. Nokia can make these solutions globally ubiquitous rapidly.

What's in it for Nokia? Nokia could become the most important and valuable company in the world. And do the greatest public service.

NOKIA

Proof of technology

- **White House Office of Science and Technology Policy** Member of the Provenance Group of the First National Cyber Leap Year Summit
- **United Nations International Telecommunications Union** presentation
- **Security Analysis** – University of California Berkeley
- **Performance Analysis** – University of Victoria, British Columbia
- **Unbroken** in “The $200,000 Challenge That Black Hat Would Not Take”
- Consul General of Canada & CTA brings WNL to Cambridge Innovation Center –MIT

--

All presentations can be viewed at www.wnlabs.com > Technology tab > YouTube video

- YouTube WN Key creation and speed video Demo
- Prove it yourself. Download FREE WN Email Attachment Encryptor – WN Key Creation and Speed test
- Whitenoise Technologies are patented globally : US, EU., China, India, Canada, Brazil etc.

Key asks from Nokia

Q: How does Nokia fit a 400 quadrillion byte one-time-pad on a cell phone? A: **The Whitenoise algorithm**

Q: How does Nokia provide complete network security (not just encryption) with a single key? A: **The DIVA protocol**

Q: How does Nokia build completely secure network frameworks? **The DDKI virtual framework**

Q: Does Nokia have to replace or get rid of anything? A: **No**

--

WNL is asking Nokia to become its key partner for funding, joint solution development, technology partnering, reselling and licensing to operators, being a customer, and/or acquisition.

WNL is asking Nokia to talk business and vision. Together we can make the entire suite of Microsoft services and products secure for each client with a single key given one time with Nokia smart phones as the foundation.

Nokia and WNL can change the world, make it safer and have unlimited business opportunities and unlimited revenue while doing so.

NOKIA

- no cyber crime
- no fear
- no hassle
- no competitors
- no manufacturing
- no doubt

Home office
#701 – 1736 W. 10th St.
Vancouver, British Columbia
Canada V6J 2A6

NOKIA

Canadian Cyber Security Accelerator
Cambridge Innovation Center
Kendall Square MIT
101 Main St. Cambridge Ma. USA 02142

- no time to waste
- no time to hesitate
- no brainer