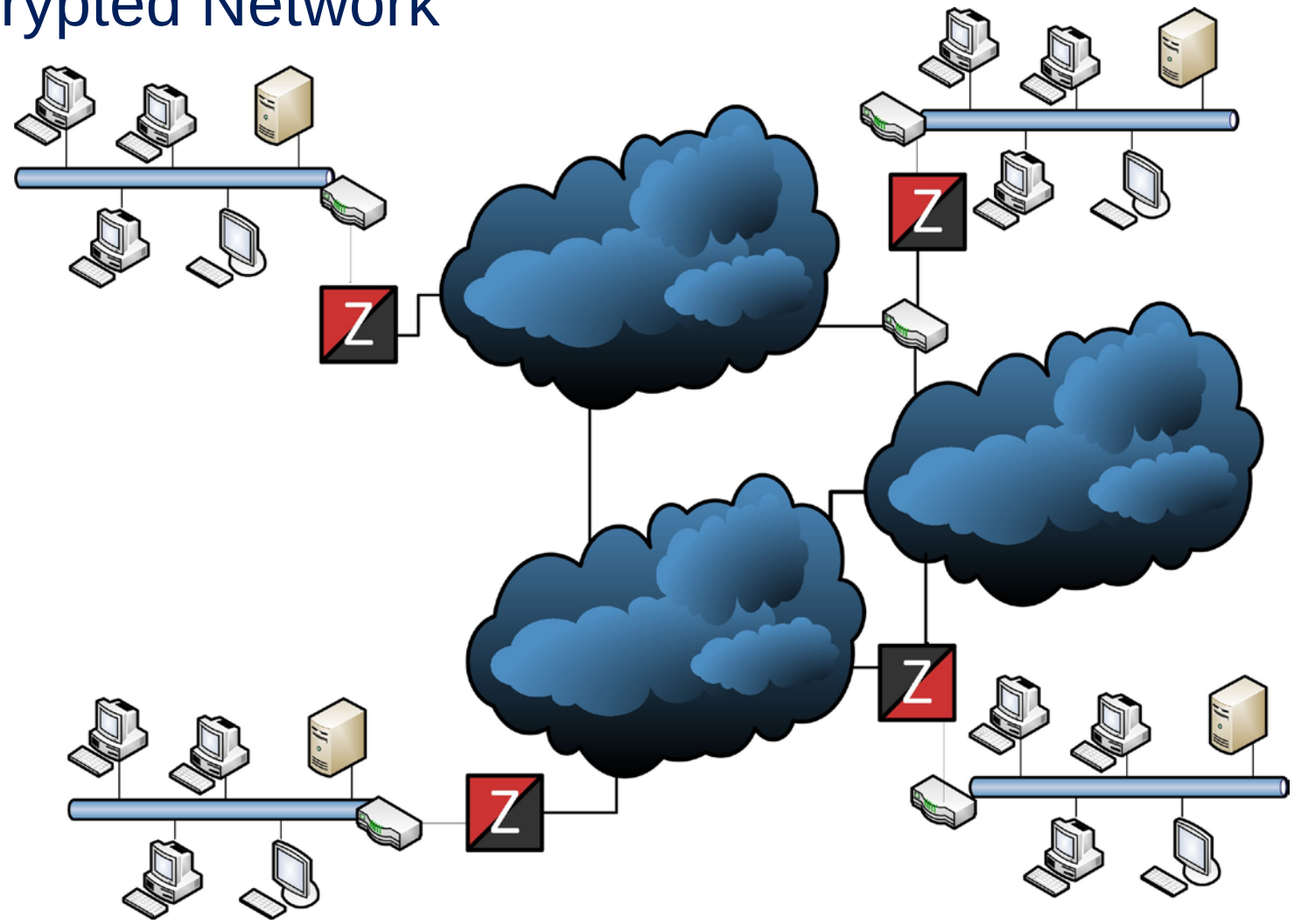
The All-Encrypted Network and the Cyber Threat

DEFENCE AND SPACE

Professor Brian Turton
March 2019

AIRBUS

An All-Encrypted Network



Security

- Confidentiality
  - The property that information is not made available or disclosed to unauthorised individuals, entities or processes.
- Integrity
  - The property of safeguarding the accuracy and completeness of assets – this may include the ability to prove an action or event has taken place, such that it cannot be repudiated later.
- Availability
  - The property of being accessible and usable upon demand by an authorised entity.

Impact Level

A Business Impact Level is a numeric indicator of the level of impact likely to result from the compromise of Confidentiality, Integrity or Availability of an asset. It is a seven point scale ranging from IL0 (no impact) to IL 6 (maximum impact).

Impact Level

1.Minimal delay to or loss of minor supply service

2.Loss of a number of minor supply services

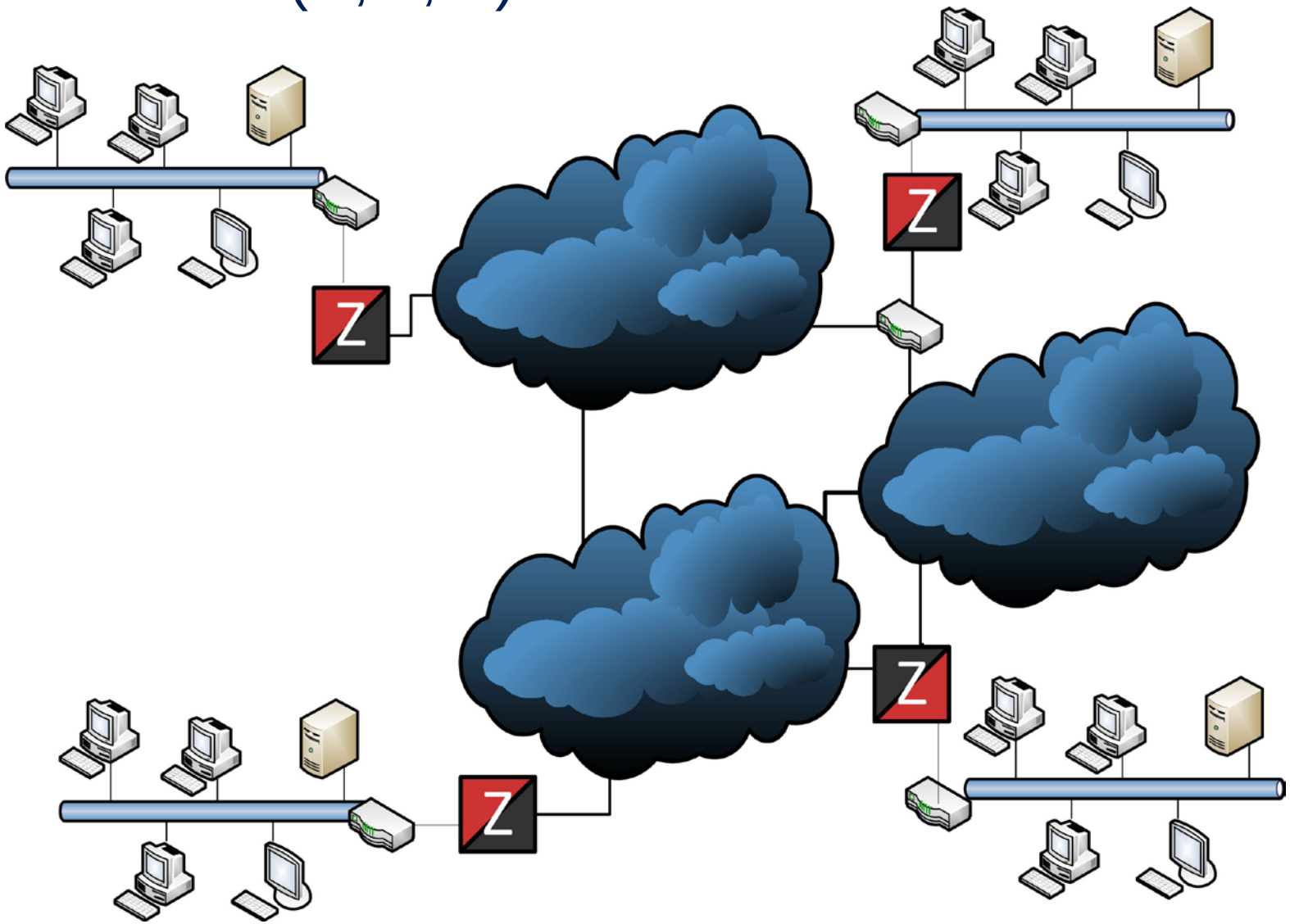
3.Make it more difficult to maintain the operational effectiveness or security of UK or allied forces
(e.g. compromise of UK forces training materials or supply procedures)

4.Cause damage to the operational effectiveness or security of UK or allied forces
(e.g. compromise of a logistics system causing re-supply problems without causing risk to life)

5.Cause severe damage to the operational effectiveness or security of UK or allied forces
(e.g. compromise of the operational plans of units of company size or below in a theatre of military operations)

6.Cause exceptionally grave damage to the operational effectiveness or security of UK or allied forces
(e.g. compromise of the operational plans of units of battalion size or above in a theatre of military operations)

Apply Impact levels (C, I , A)



Confidentiality

The property that information is not made available
or disclosed to unauthorised individuals, entities or processes

AIRBUS

An emxpale of ofubscatoin taht deos not wrok

Just because something is obscured it does not mean it does not contain information

“Aoccdrnig to a rscheearch at Cmabrigde Uinervtisy,
it deosn't mttaer in waht oredr the ltteers in a wrod are,
the olny iprmoetnt tihng is taht the frist and lsat ltteer be at the rghit pclae.
The rset can be a toatl mses and you can sitll raed it wouthit porbelm.
Tihs is bcuseae the huamn mnid deos not raed ervey lteter by istlef,
but the wrod as a wlohe.”

The protection of information other than the content is ‘Traffic Flow Security’

Traffic Flow Security

Questions

- Who is communicating?
- Where are they located?
- What are they doing?
- What are they looking at?
- How soon before they take action?
- Who will be taking action?

Information

- Packet Size
- Packet timing
- Packet rates/counting
- Communication patterns/direction
- IP addresses
- DiffServCodePoint
- Reaction to deleted or delayed packets

Lessons from History

World War 2

Using

- Direction finding
- Signatures of Radios
- Call signs

Determine

- Order of battle
- Intentions
- Units

In the Second World War, traffic analysis was used by the British at Bletchley Park to assess the size of Germany's air-force, and Japanese traffic analysis countermeasures contributed to the surprise of their 1941 attack on Pearl Harbour.

Nowadays, Google uses the incidence of links to assess the relative importance of web pages, credit card companies examine transactions to spot fraudulent patterns of spending, and amateur plane-spotters revealed the CIA's `extraordinary rendition‘ programme.

Diffie and Landau, in their book on wiretapping, even went so far as to say that traffic analysis, not cryptanalysis, is the backbone of communications intelligence

Intelligence Power in Peace and War

Michael Hermann, who has served as chair of the UK Joint Intelligence Committee, describes the value of extracting data from non-textual sources (not the content)

“These non-textual techniques can establish
targets' locations,
- order-of-battle
- and movement.

Even when messages are not being deciphered, traffic analysis of the target's C3I system and its patterns of behaviour provides indications of his
- intentions
- and states of mind,

in rather the same way as a neurologist develops insights about a silent patient by studying EEG traces from the brain.

Traffic Flow Security Research

Attack

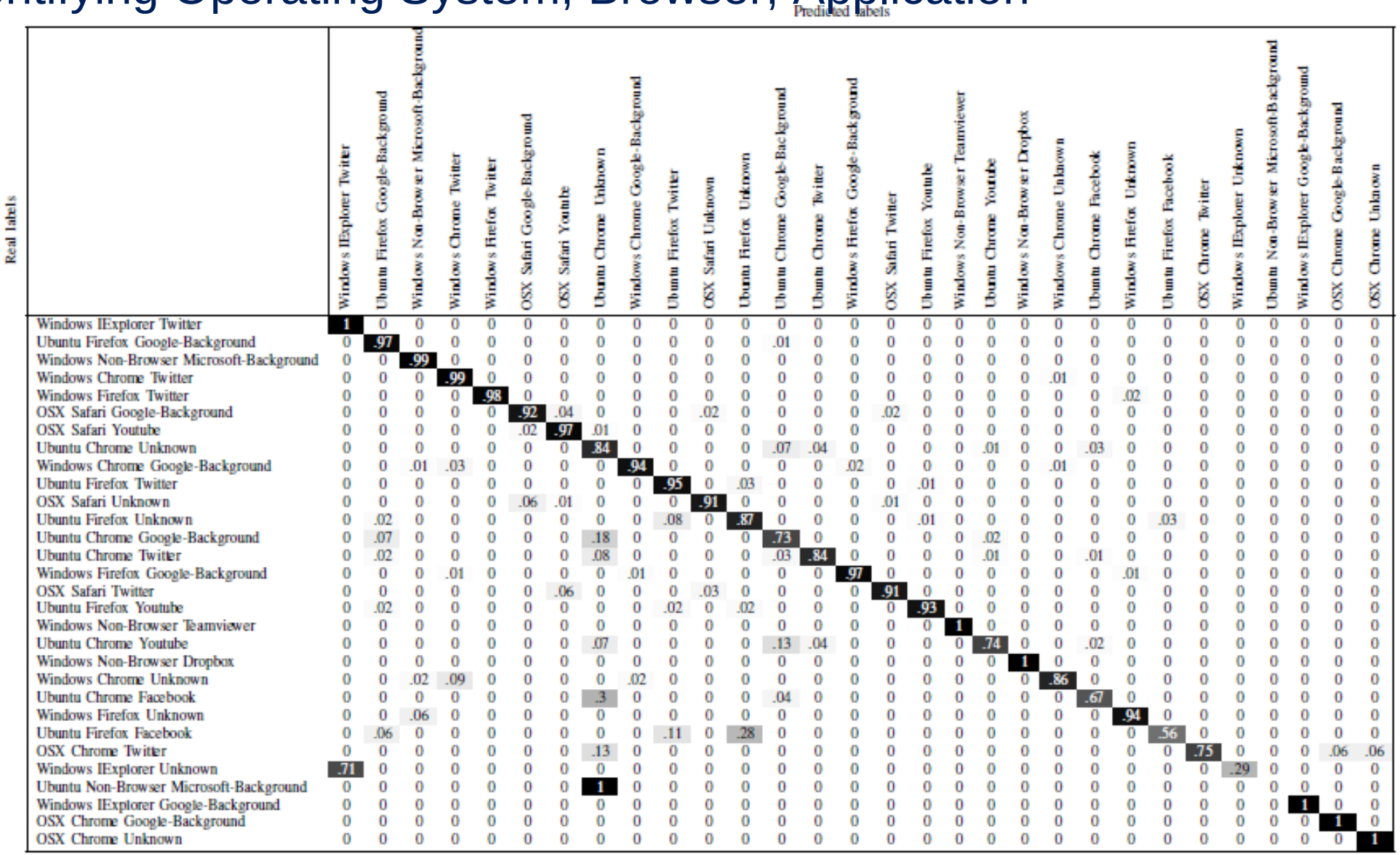
- Finger printing websites (pattern of TCP flows/packets and sizes)
- Identifying applications and operating systems (pattern of flows and communication flow configuration)
- Identifying source and destination (TOR scenario)
- Identifying language
- Identify the network topology
- Identify geographic location

Defence

Statistics modification or obfuscation

- packet size,
- flow size/direction,
- web object size/number
- timing

Identifying Operating System, Browser, Application



AIRBUS

Real Time Traffic Classification Example

Algorithm	Http	SMTP	POP3	Skype	EDonkey	BT	Encrypted BT	RTP	ICQ
k-means	0.78	0.93	0.93	0.85	0.80	0.75	0.74	0.93	0.71
k-NN	0.997	0.999	1.0	0.945	0.947	0.96	0.98	0.997	0.962
hybrid	0.997	0.999	0.998	0.94	0.94	0.963	0.974	0.992	0.954

Client number of packets; Server number of packets; Total number of packets;
Client packet size expectation; Server packet size expectation;
Client average ‘packets per second’ rate; Server average ‘packet per second’ rate;
Client packet size variance; Server packet size variance;
Total client bytes; Total server bytes; Download to upload ratio;
Server average number of bytes per bulk;
Client average number of bytes for bulk; Server average number of packets for bulk;
Client average number of packets for bulk; and Transport protocol (TCP or UDP)

Markov Chain Fingerprinting

	Campus1		Campus2		Campus4	
Application	TPR	FPR	TPR	FPR	TPR	FPR
Twitter	0.932	0.007	0.908	0.04	0.907	0.018
Dropbox	0.692	0.01	0.704	0.005	0.922	0.01
Gadu-Gadu	0.97	0.004	0.916	0.004	0.781	0007
Mozilla	0.001	0.028	0.0	0.023	0.405	0.041
MBank	0.02	0.006	0.0	0.007	0.817	0.018
PKO	0.597	0.005	0.537	0.004	0.595	0.035
Dziekanat	0.966	0.093	0.933	0.012	0.988	0.0
Poczta	0.942	0.002	0.967	0.004	0.97	0.0
Amazon S3	0.978	0.146	0.991	0.111	0.996	0.0
Amazon EC2	0.02	0.007	0.035	0.084	0.579	0.013

Inferring Protocols

In addition to helping profile a pattern of communications
this may also allow someone to determine if prohibited protocols are being disguised as HTTP

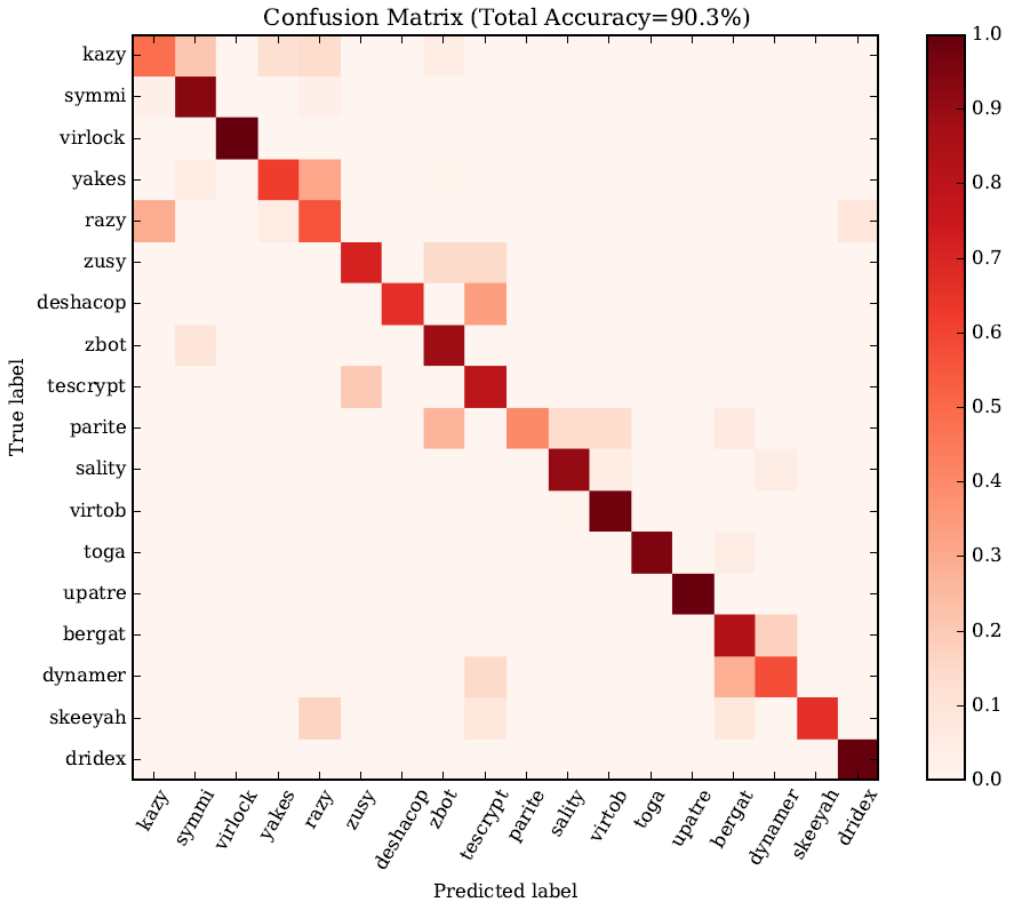
Classification Probability									
Protocol	AIM	SMTP-out	SMTP-in	HTTP	HTTPS	FTP	SSH	Telnet	none
AIM	80.8	2.9	1.4	1.6	3.1	0.9	5.4	3.2	0.7
SMTP-out	7.1	73.2	6.9	1.2	1.9	2.3	1.9	5.2	0.3
SMTP-in	2.5	10.6	77.2	0.1	0.2	4.6	0.8	3.9	0.1
HTTP	0.7	0.3	0.1	90.3	6.4	0.3	1.3	0.4	0.1
HTTPS	0.9	0.8	0.1	5.9	88.5	0.6	1.9	0.8	0.5
FTP	7.1	4.1	11.1	0.9	2.1	57.7	6.0	11.0	0.0
SSH	3.4	1.8	9.3	1.5	6.8	2.8	69.1	1.9	3.2
Telnet	2.2	1.0	1.8	3.5	2.2	2.6	3.2	82.9	0.4

Spotting Encrypted Malware

Four machine learning classifiers were trained using different subsets of data features.

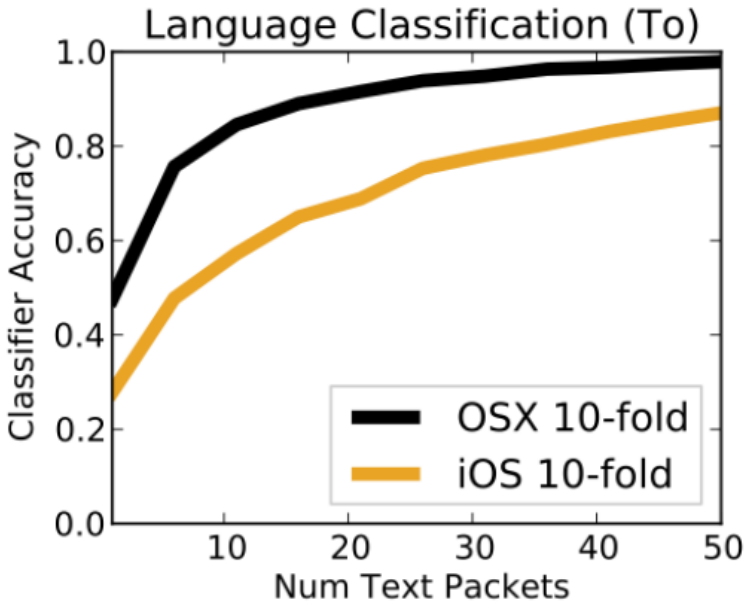
1) Flow metadata (Meta), the sequence of packet lengths and inter-arrival times (SPLT), and the distribution of bytes (BD),
2) TLS information (TLS),
3) As the 1) plus the TLS client information, (the offered ciphersuites, advertised extensions, and the client's public key length).
4) All data, and an additional, custom feature: whether the server certificate was self-signed (SS).

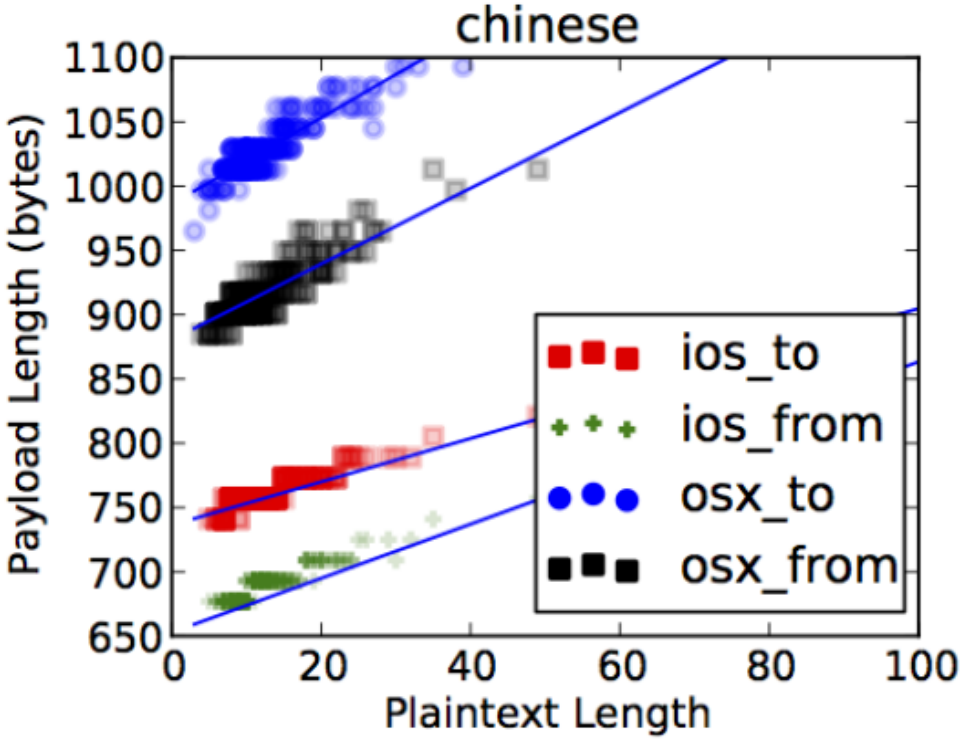
Malware Family	Meta+SPLT +BD	TLS Only	Meta+SPLT +BD+TLS	All+SS
Bergat*	100.0%	100.0%	100.0%	100.0%
Kazy*	98.5%	99.5%	99.8%	100.0%
Parite*	99.3%	97.8%	99.6%	99.6%
Sality*	95.0%	94.1%	97.7%	98.0%
Tescrypt*	89.8%	95.6%	97.6%	97.6%
Upatre*	99.9%	98.7%	100.0%	100.0%
Virtob*	99.2%	98.8%	99.4%	99.4%
Yakes*	88.7%	98.5%	99.7%	99.7%
Zbot*	98.9%	99.6%	99.7%	100.0%
Zusy*	98.6%	88.7%	99.9%	99.9%
Deshacop	93.0%	63.6%	96.1%	96.1%
Dridex	16.5%	68.7%	78.5%	97.9%
Dynamer	95.4%	78.8%	95.7%	96.5%
Razy	91.5%	77.1%	95.9%	96.8%
Skeeyah	95.9%	82.1%	98.6%	98.6%
Symmi	99.1%	92.4%	99.8%	99.8%
Toga	100.0%	100.0%	100.0%	100.0%
Virlock	100.0%	100.0%	100.0%	100.0%

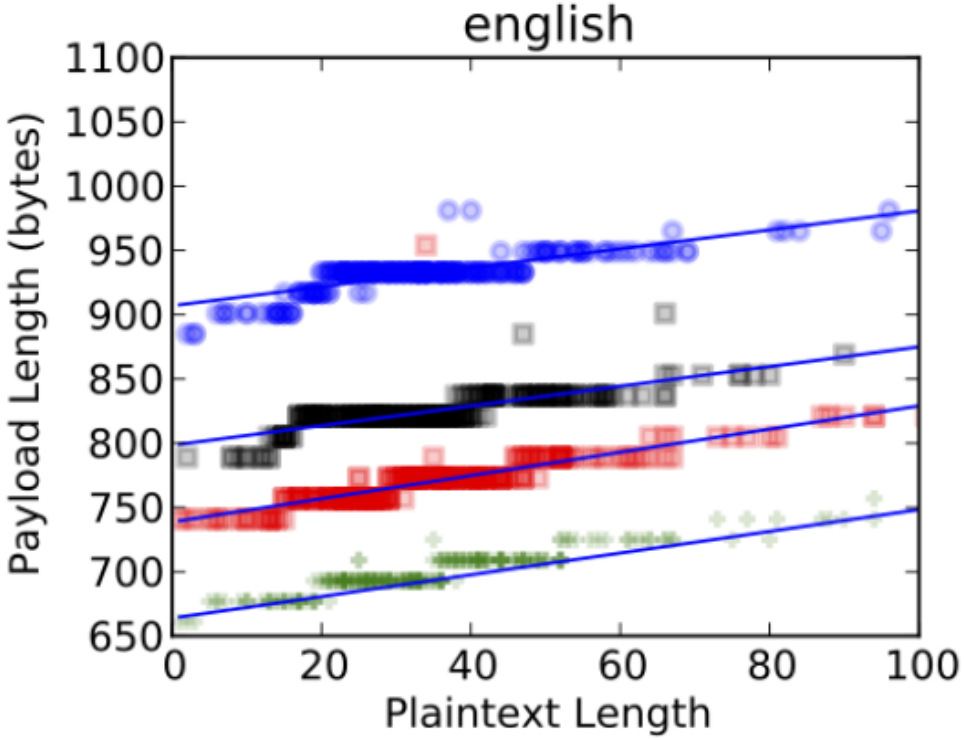


AIRBUS

Language Classification in Messages







AIRBUS

Padding Defence

	Percentage Overhead	
Countermeasure	LL	H
Session Random 255	9.0	7.1
Packet Random 255	9.0	7.1
Linear (128 multiple)	4.2	3.4
Exponential (factor 2)	8.7	10.3
Mice-Elephants (128 or MTU)	41.6	39.3
Pad to MTU	81.2	58.1
Packet Random MTU	40.1	28.8
Direct Target Sampling	86.4	66.5
Traffic Morphing	60.8	49.8

		LL	H	P
$k = 2$	Type-1	85%	71%	99%
	Type-2	97%	80%	99%
	Type-3	98%	76%	99%
$k = 128$	Type-1	41%	13%	91%
	Type-2	46%	5%	90%
	Type-3	25%	3%	82%

Voice over IP

Attack

- Identification of the existence of hidden voice flows (0.9) and specific speech(0.98)
- Uncovering Spoken Phrases (Scenario dependent)
- Identification of speaker (~48%)
- Identification of Language (55-100%)

Voice Coding Types

- Constant Bit Rate
- Variable Bit Rate
- Voice Activation Detection (Silence Suppression hangover of 20-70ms)

Lessons from History - Acoustic

Keyboard Acoustic Emanations

Raw

the big money fight has drawn the shoporo od dosens of companies in the entertainment industry as well as attorneys gnnerals on states, who fear the fild shading softwate will encourage illegal acyivitt, srem the grosth of small arrists and lead to lost cobs and dimished sales tas revenue.

After trigram decoding

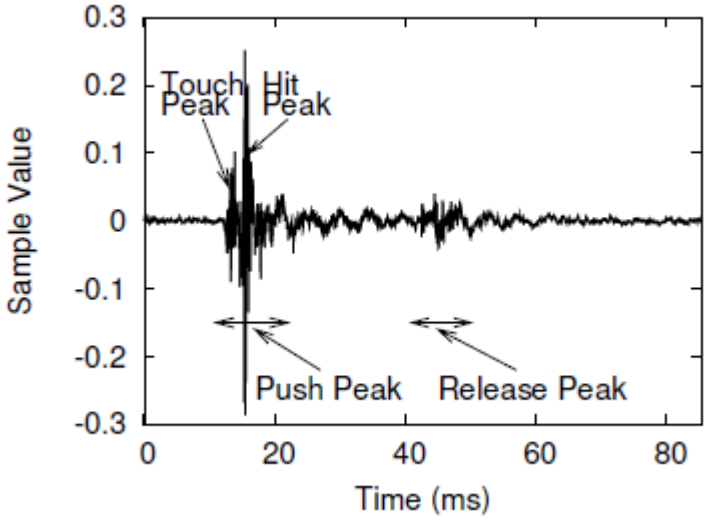
the big money fight has drawn the support of dozens of companies in the entertainment industry as well as attorneys generals in states, who fear the film sharing software will encourage illegal activity, stem the growth of small artists and lead to lost jobs and finished sales tax revenue.

Original

the big money fight has drawn the support of dozens of companies in the entertainment industry as well as attorneys gnnerals in states, who fear the file sharing software will encourage illegal activity, stem the growth of small artists and lead to lost jobs and dimished sales tax revenue.

Results Before language correction Words ~58%, Chars ~88%

After language correction Words ~80%, Chars ~92%



History

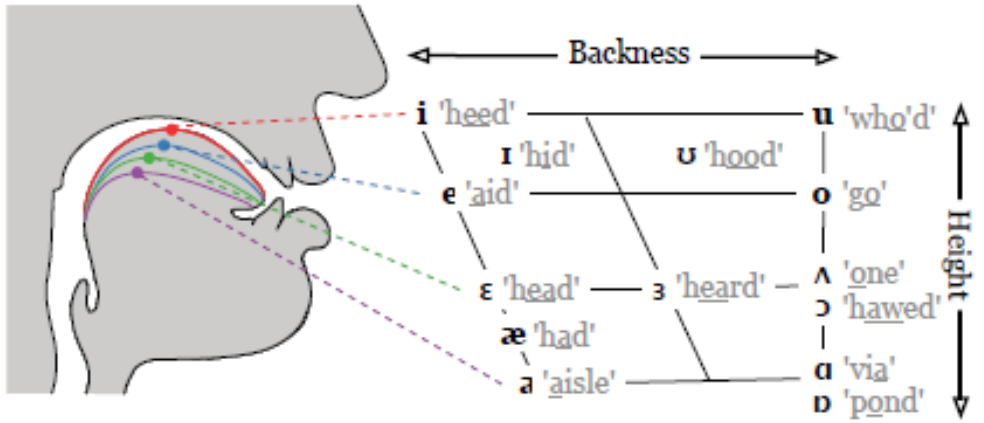
Radio listening stations would recognise operators by their distinctive ‘fist’ when tapping Morse. This gave vital clues as to where units were being assigned.

Acoustic keyboard emanations have been reported as being used by the CIA

Uncovering Spoken Phrases in Encrypted Voice over IP Conversations (VBR using phonemes)

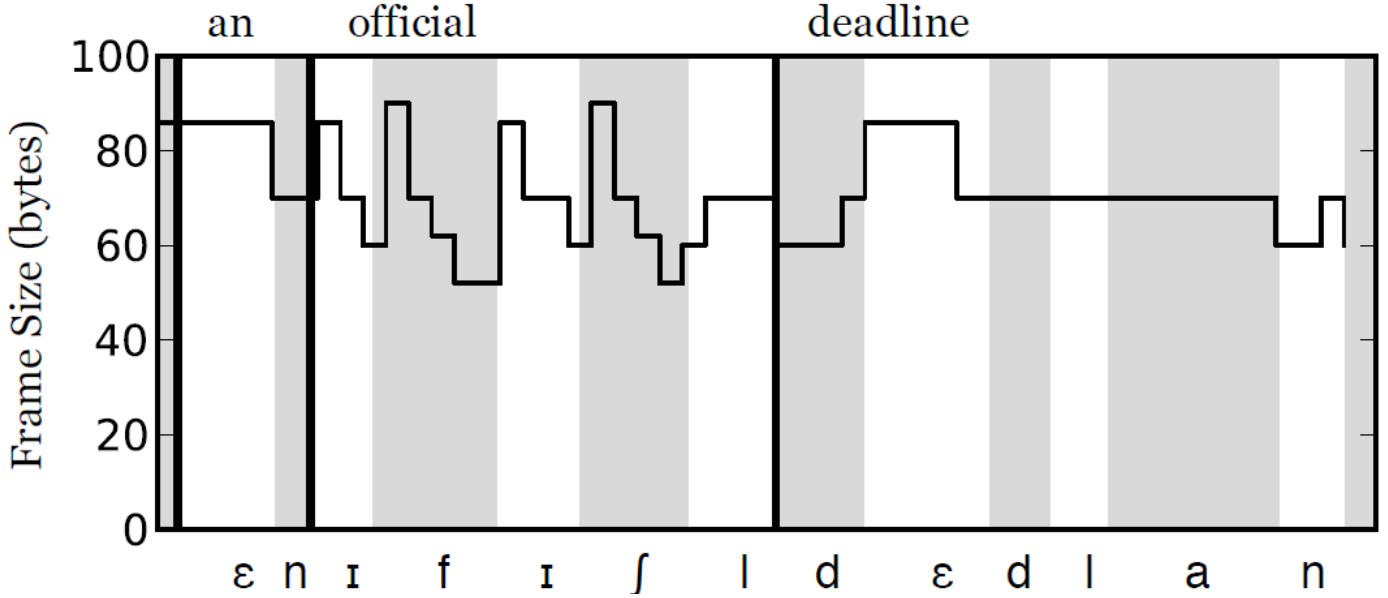
Bit rate and position in sequence for each packet fingerprints the word

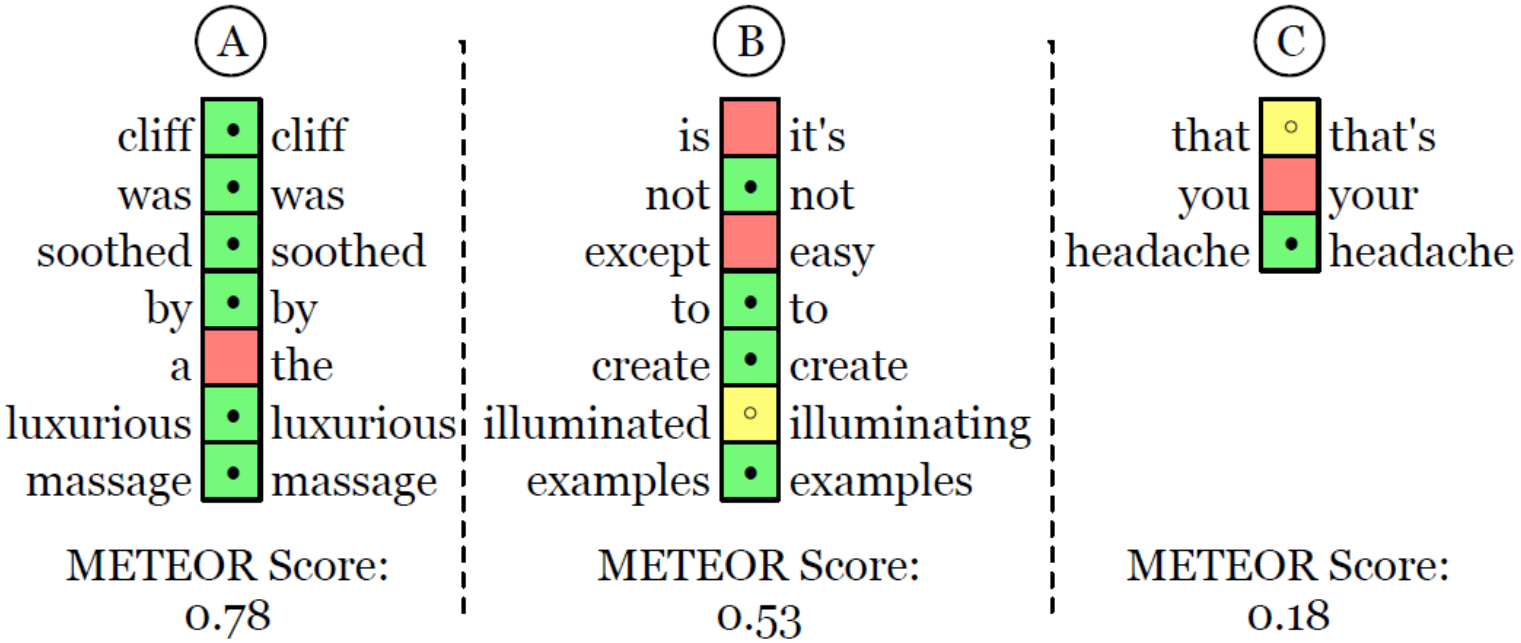
Phrase	Area
Young children should avoid exposure to contagious diseases.	0.98
Even a simple vocabulary contains symbols.	0.96
Military personnel are expected to obey government orders.	0.95
Cory and Trish played tag with beach balls for hours.	0.92
Youngsters love common candy as treats.	0.92
Weather-proof galoshes are very useful in Seattle.	0.89
Don't ask me to carry an oily rag like that.	0.89
Ralph controlled the stopwatch from the bleachers.	0.00
The best way to learn is to solve extra problems.	0.00
The bungalow was pleasantly situated near the shore.	0.00
The emblem depicts the acropolis all aglow.	0.00
The fish began to leap frantically on the surface of the small lake.	0.00
The morning dew on the spider web glistened in the sun.	0.00
The sound of Jennifer's bugle scared the antelope.	0.00



AIRBUS

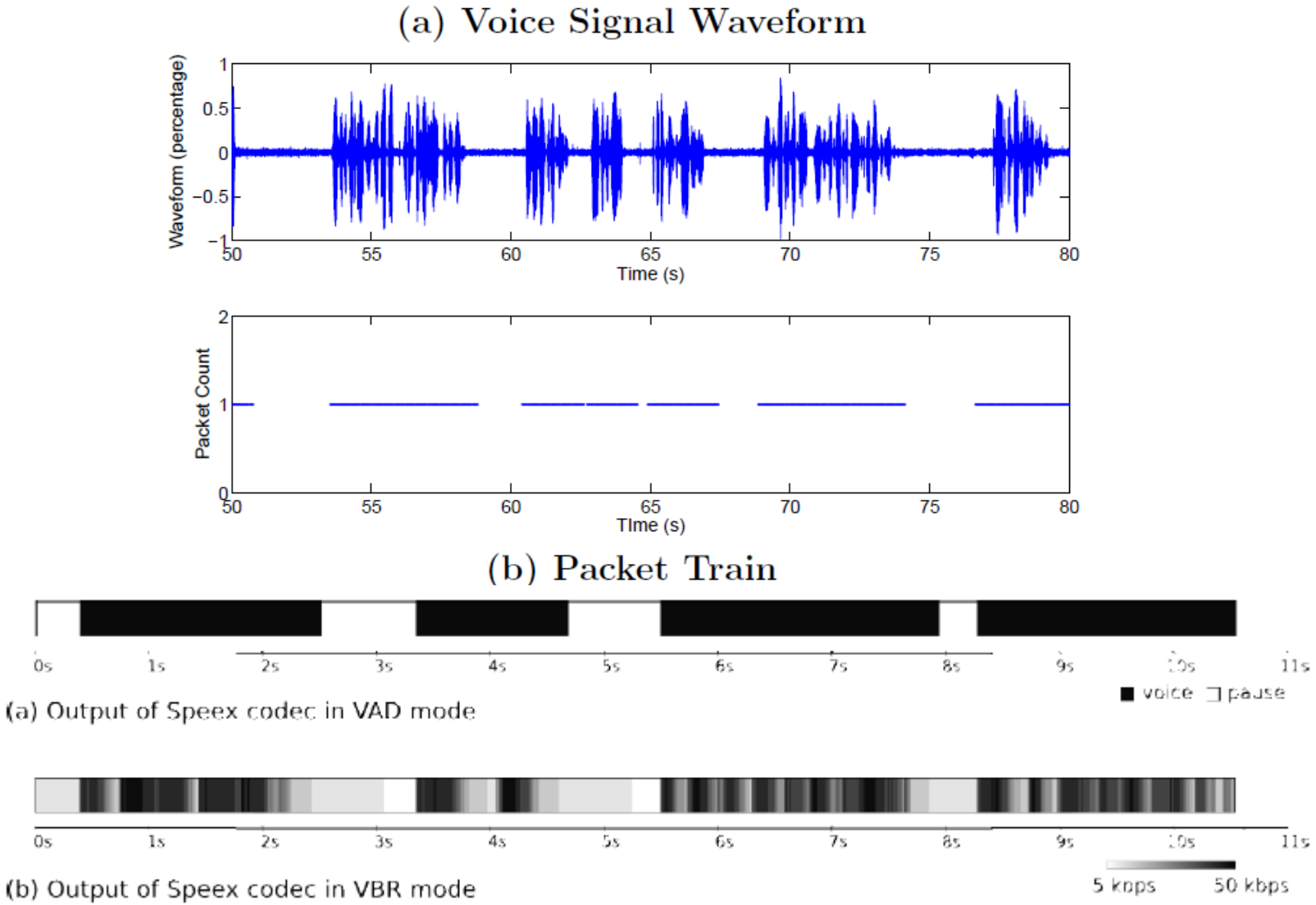
VoIP Example



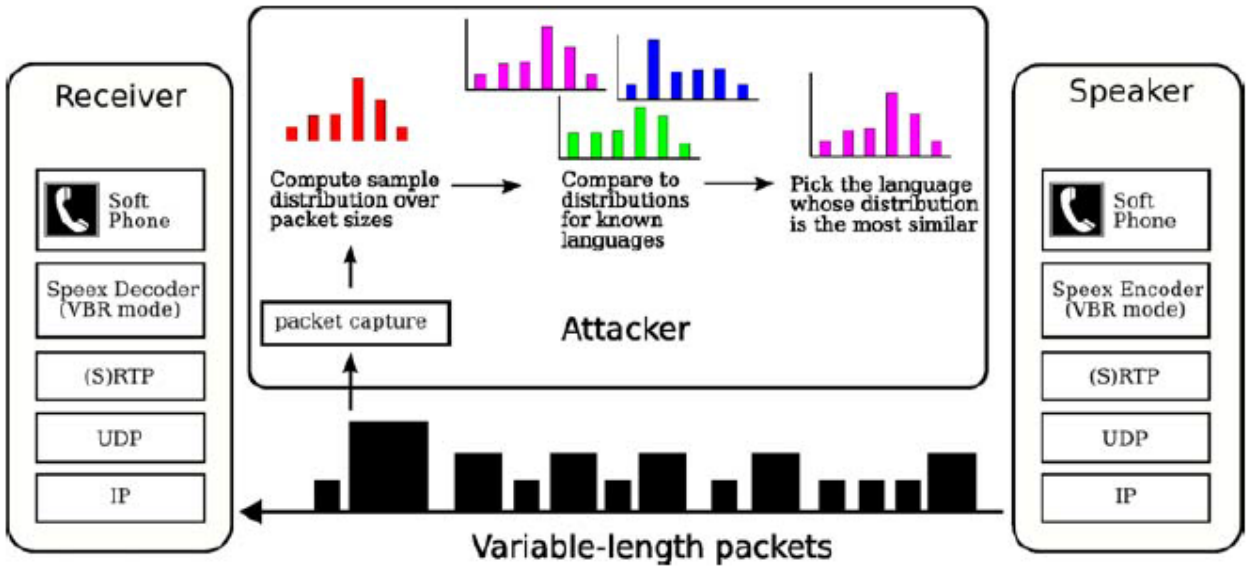


AIRBUS

Voice information from Silence Suppression

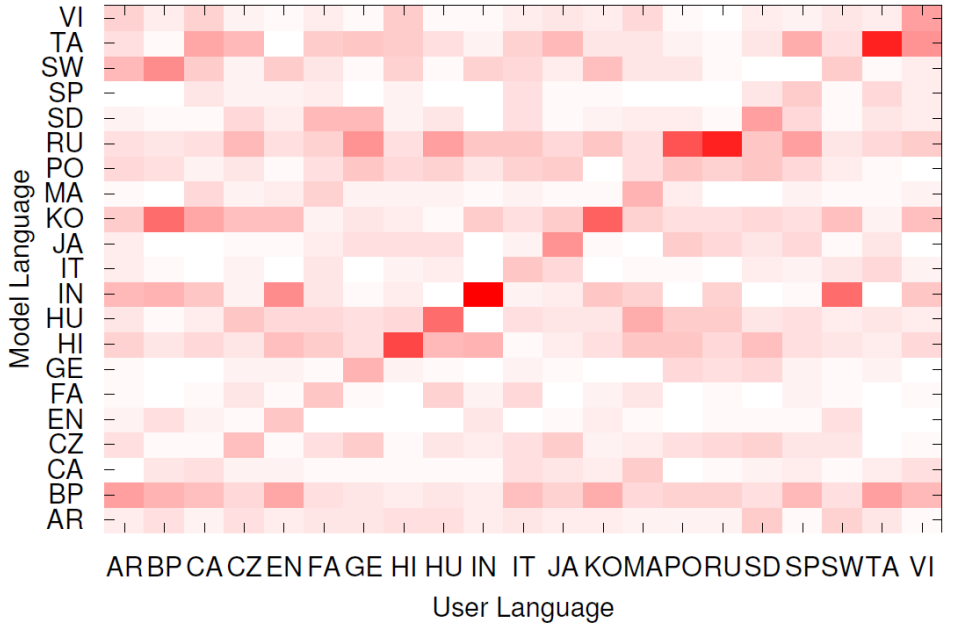


Language Classification



Lang.	Acc.	Lang.	Acc
EN-FA	0.980	CZ-JA	0.544
GE-RU	0.985	AR-SW	0.549
FA-SD	0.990	CZ-HU	0.554
IN-PO	0.990	CZ-SD	0.554
PO-RU	0.990	MA-VI	0.565
BP-PO	0.995	JA-SW	0.566
EN-HI	0.995	HU-VI	0.575
HI-PO	0.995	CZ-MA	0.580
BP-KO	1.000	CZ-SW	0.590
FA-PO	1.000	HU-TA	0.605

Confusion Matrix: All Languages



AIRBUS

Integrity

The property of safeguarding the accuracy and completeness of assets – this may include the ability to prove an action or event has taken place, such that it cannot be repudiated later.

AIRBUS

Integrity

We understand how (using mathematical functions) to ‘sign’ data securely.

Issues

- Trusting the hardware/software doing the signing to implement the Security Enforcing Function properly
- Trusting the hardware/software not to modify what the author provided
- Authenticating the author to the hardware
- Spoofing

Authentication

- What you are (biometrics),
- What you know (pass-phrase/word/pattern),
- What you have (token).

In recent years their has been more thought put into authentication approaches which support the human and disadvantage the machine.

At the security domain level the IP-encryptors can provide basic integrity.

Availability

The property of being accessible and usable upon demand by an authorised entity.

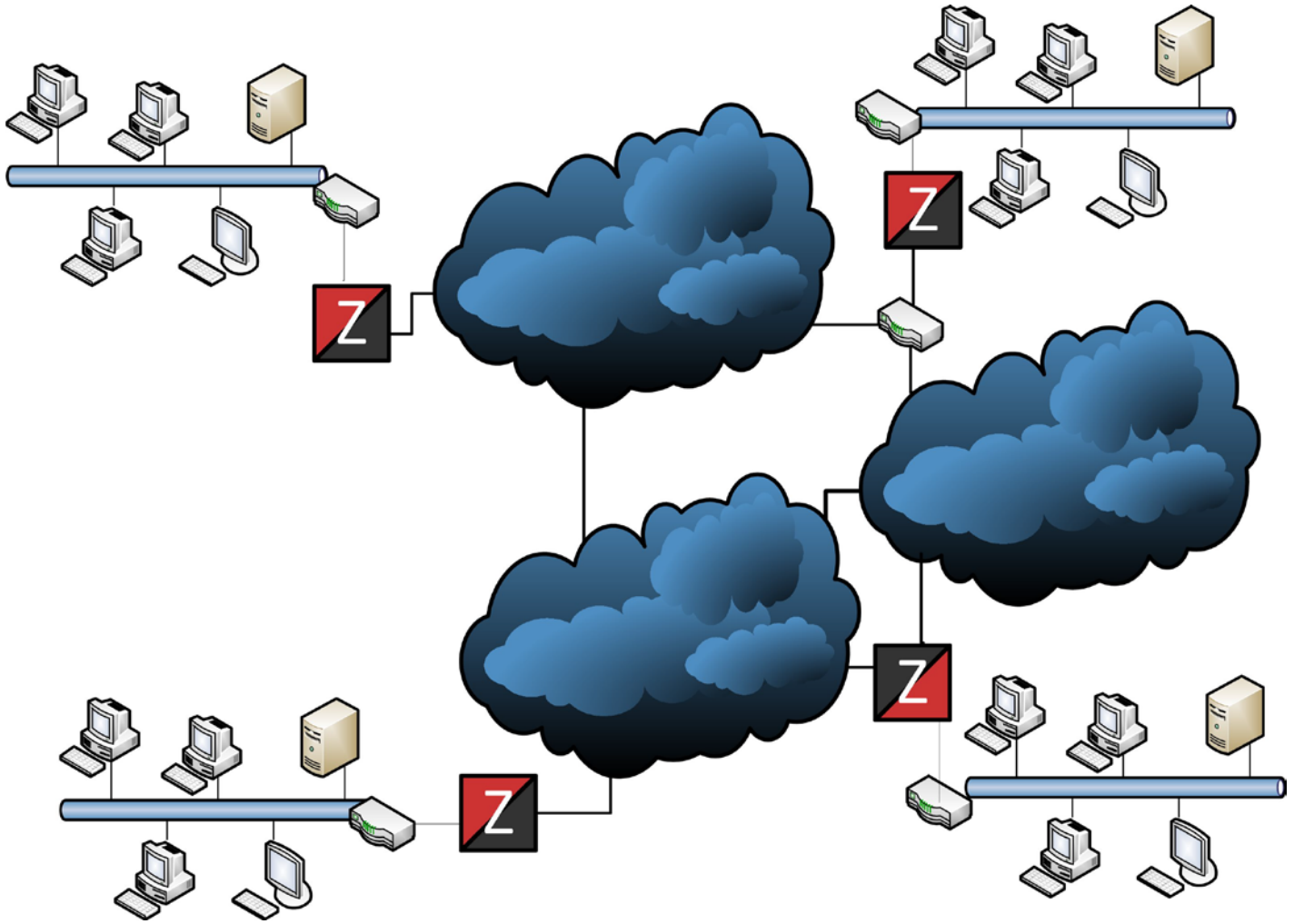
AIRBUS

Availability Issues

- Individual component networks may not be trusted to the same level and so some control is needed.
- Ensuring that only appropriate information is passed (Encrypted packets, Routing traffic, RSVP?).
- Recognising and reacting to a compromised network in a timely manner
  (some aspects may be very subtle).
- Ensuring critical traffic follows reliable routes (problematic as it is encrypted).
- Having a management system to support availability without introducing unacceptable levels of vulnerability (potential cross-domain issues).
- Intrusion Detection/Protection when packet inspection is prevented by crypto
- Traffic Policing and Shaping when packet inspection is prevented by crypto
- Performance Enhancing Proxies and WAN Accelerators are disabled by crypto

This is an area which needs careful consideration

Aid to Discussion



Summary

Confidentiality

- Traffic Flow Security is a significant issue if you cannot control your applications or apply specialist measures and you wish to send encrypted flows over an untrusted network.
- If you apply specialist measures it may harm the performance of the network

Integrity

- At a security domain level, this is well supported
- At a user level, there is reasonable support through passwords, tokens and potentially biometrics
- At a user device level, trust in the device and its software to support integrity becomes an issue if it must be high level

Availability

In an all-encrypted network there are numerous availability issues around

- IPS/IDS
- PEPs and WAN accelerators
- Routing of critical traffic
- Protection of component networks from each other
- Management to support availability

Thank you

AIRBUS